Lecciones populares de matemáticas

CRITERIOS DE DIVISIBILIDAD

N. N. Vorobiov

$$a_1 + a_2 + \ldots + a_n \vdots b$$

Editorial MIR  Moscú



ИЗДАТЕЛЬСТВО
МИР

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ

Н. Н. ВОРОБЬЕВ

ПРИЗНАКИ ДЕЛИМОСТИ

ИЗДАТЕЛЬСТВО «НАУКА»
МОСКВА

LECCIONES POPULARES DE MATEMÁTICAS

N. N. VOROBIOV

CRITERIOS DE DIVISIBILIDAD

SEGUNDA EDICIÓN AMPLIADA Y MODIFICADA

EDITORIAL MIR
MOSCÚ

Traducido del ruso por el ingeniero
J. Julio

Primera edición 1975
Segunda edición 1984

Impreso en la URSS

На испанском языке

ÍNDICE

Prefacio
§ 1. Divisibilidad de los números 10
§ 2. Divisibilidad de sumas y productos 26
§ 3. Criterios de residuos equivalentes y divisibilidad 32
§ 4. Criterios generales de residuos equivalentes y de divisibilidad 49
§ 5. Divisibilidad de potencias 53
Demostraciones de los teoremas 61
Resoluciones de los problemas 72

PREFACIO

QUE EL AUTOR ACONSEJA LEER CON SUMA ATENCIÓN

La actual enseñanza escolar de las matemáticas se orienta fundamentalmente a desarrollar en el alumno el pensamiento funcional, y capacitarlo para operar con objetos matemáticos continuos. Los cambios que se planean en los programas escolares de esta materia están encauzados en la misma dirección. Al mismo tiempo, últimamente, se investigan nuevos campos de aplicación de las matemáticas: la composición de programas para computadoras, algunos aspectos de la cibernética y el estudio de operaciones, economía matemática, lingüística matemática, etc. El dominio de estas ramas de la ciencia, junto con el perfeccionamiento del aparato clásico, exige el desarrollo de la técnica combinatoria, el análisis de lo discreto y la creación de nuevas abstracciones fructíferas. Los aspectos enumerados de las matemáticas también deberán ilustrarse en la literatura de divulgación científica.

Desde la linde a la espesura de un bosque conducen muchos senderos. Son sinuosos, se juntan, se separan de nuevo y se cruzan. Paseando podemos notar su gran cantidad, recorrer algunos de ellos y ver cómo se internan en las frondas. Si se quiere estudiar seriamente un bosque es necesario seguir sus senderos mientras se puedan distinguir entre la pinocha seca y las pequeñas matas de arándano. Para poder aprovechar los dones del bosque hay que abandonar por completo los caminos trillados y abrirse paso a través del entrelazamiento de ramas espinosas.

El presente folleto puede considerarse como descripción de uno de los posibles paseos por la linde de las matemáticas contemporáneas. La exposición de los datos básicos, referentes a los criterios de divisibilidad, nos obliga a incluir en este folleto algunas cuestiones bastante abstractas de las matemáticas discretas. A éstas pertenecen, ante todo, las afirmaciones de la teoría elemental de los números, agrupadas en torno al teorema fundamental de la aritmética y al análisis de la descomposición canónica de un número natural en factores simples. Luego, la propia divisibilidad de los números se examina como una relación definida en el conjun-

to de los números enteros, es decir, como la realización de una noción bastante general y abstracta. Por último, los criterios de divisibilidad se tratan aquí como algoritmos que transforman cada cifra en respuesta a la interrogación ¿se divide o no por el número dado? El autor consideró útil destacar entre los criterios de divisibilidad los «criterios de equirresidualidad o residuos equivalentes» que transforman los números en residuos al dividirlos por un número dado.

Con objeto de acentuar las variadas relaciones mutuas entre hechos matemáticos sueltos y las posibilidades de diferentes enfoques de un mismo tema, algunas afirmaciones se establecen de dos maneras diferentes.

El libro está destinado a los escolares de los grados superiores aficionados a las matemáticas y (a excepción de algunas menciones de la fórmula del binomio) no exige ningún conocimiento previo, excepto capacidad para efectuar sencillas transformaciones idénticas. Pero la estructura lógica del material es bastante compleja, por lo que la asimilación del mismo en todos sus detalles exige mucha atención y paciencia.

Recomendamos al lector el siguiente plan de estudio del libro.

En la primera lectura puede limitarse solamente al texto básico §§ 1—4 sin resolver los problemas (a excepción de los №№ 31, 34, 36, 45, 47, 49 y 50). Esto dará un conocimiento descriptivo general de la materia. Como la mayoría de la gente sin experiencia en matemáticas está convencida de la exactitud del teorema de descomposición unívoca de un número natural en factores primos (considerándolo por lo visto, como un axioma), ella puede entender los teoremas 9—13 como sus consecuencias.

En la segunda lectura es necesario tratar de demostrar por sí mismo todos los teoremas en el orden en que se presentan. Para que el lector no ceda demasiado frecuentemente a la tentación de utilizar las demostraciones ya hechas de los teoremas, todas ellas fueron insertadas en un apartado especial. Una excepción viene a ser la demostración del teorema 7, llamada a servir de diapasón que prepare al lector ya, desde la primera lectura, al nivel necesario de rigurosidad,

En la segunda lectura conviene estudiar el § 5 y resolver también los problemas del texto básico.

Por último, en la tercera lectura se estudia lo que está en gallarda y los problemas que contiene.

El que desee profundizar sus conocimientos en el campo de la teoría de los números deberá recurrir al curso clásico del académico I. M. Vinográdov «Fundamentos de la teoría de los números» (Editorial Mir, 1977).

Se recomienda estudiar la teoría abstracta de las relaciones en un conjunto y las sucesivas cuestiones vinculadas a él por el libro «Lecciones de álgebra general» de A. G. Kurosh (Ed. Naúka, 1973) o la «Teoría de las estructuras» de G. Birkhoh (IL, 1951).

Por fin, el folleto «Algoritmos y resoluciones de problemas con computadoras» de B. A. Trajtenbrot (Fismatguiz, 1960) contiene una explicación más detallada y sistemática de la noción algorítmica, y en la monografía básica «Teoría de los algoritmos» (Trabajos matemáticos del Instituto Steklov de la Academia de Ciencias de la URSS, t. 42, 1954) de A. A. Márkov hallamos una exposición rigurosa del tema.

La segunda edición se diferencia de la primera solamente por algunos mejoramientos de redacción. El autor agradece al profesor Grella (RDA) por la ayuda prestada en este asunto.

N. N. Vorobiov

PREFACIO A LA PRESENTE EDICIÓN

En esta edición se explica con más detalle que en la anterior la esencia algorítmica de los criterios de equirresidualidad y divisibilidad y se incluye, además, un examen de ellos en sistemas numéricos arbitrarios.

Vyritsa
año 1979

N. N. Vorobiov

§ 1. DIVISIBILIDAD DE LOS NÚMEROS

1. La suma, diferencia y producto de dos números enteros resultan siempre enteros. Es lo que se suele llamar a veces *conjunto cerrado* de números enteros, refiriéndose a las operaciones de adición, resta y multiplicación.

Pero referido a la operación de división, este conjunto deja de ser cerrado: hablando en general, el cociente de la división de un entero por otro puede no ser entero.

Por eso, al estudiar las particularidades de la división de los enteros, una de las primeras cuestiones que se presenta trata de si es factible o no esta operación para dos números dados, es decir, de su *divisibilidad*. Al examinar las otras operaciones aritméticas con números enteros, evidentemente, tal problema no surge.

En adelante consideraremos conocidas las propiedades fundamentales de las operaciones aritméticas con números enteros, así como las elementales de las igualdades y desigualdades. Al expresar «número» vamos a entender siempre, si no se dice lo contrario, que es *entero*.

Como es habitual, los números enteros no negativos: 0, 1, 2, . . . se llamarán *naturales*. Refiriéndonos a todos ellos emplearemos el término *conjunto de todos los números naturales*.

DEFINICIÓN. El número a es divisible por el b (o lo que es lo mismo, b *divide* a a) si existe un número c tal, que $a = bc$.

Este hecho se denomina *divisibilidad* del número a por el b y se anota así $a \vdots b$.

Destacamos que la escritura $a \vdots b$ no significa una *operación* concreta que se deberá efectuar con a y b, sino determinada *afirmación* que se refiere a ellos. Según los valores numéricos que tomen a y b, la afirmación $a \vdots b$ puede ser cierta o no. Así, por ejemplo, $4 \vdots 2$ lo es y $4 \vdots 3$ no.

Para dilucidar si la afirmación $a \vdots b$ es cierta o no, es decir, para aclarar la divisibilidad del número a por el b, existen muchos y variados procedimientos. Uno de ellos consiste en dividir directamente a por b. Pero a menudo esto resulta demasiado largo y fatigoso y, naturalmente, surge el deseo de comprobar la autenticidad de la divisibilidad que nos interesa sin efectuar la división misma. Tampoco está

de más la siguiente consideracion: pór ahora nos interesa únicamente *el hecho en sí de la divisibilidad* del número a por el b; al efectuar la división, sabremos también su cociente y residuo (si la división no resulta exacta) aunque carentes de todo valor para nosotros, ya que en el momento dado sólo nos interesa saber si el residuo de la división va a ser igual o no a cero. Por consiguiente, hay motivos para suponer que efectuando la división nosotros hemos malgastado una parte de nuestro trabajo (y, por lo visto, no pequeña) en obtener «desperdicios de producción». Es de esperar procedimientos de aclaración de la divisibilidad más directos y económicos que la «burda» división, capaces de establecer el hecho de la divisibilidad por una vía más corta, sin dejar desechos tan abundantes. Estas esperanzas efectivamente se justifican, ya que tales procedimientos existen. Ellos se llaman *criterios de divisibilidad.*

Indudablemente, el lector conoce algunos de ellos. La finalidad de este libro es examinar los diferentes criterios de divisibilidad fundamentalmente en el aspecto básico.

La esencia de cualquier criterio de divisibilidad por un número dado b es que, por medio de él, la cuestión de la divisibilidad de cualquier número a por b se reduce a la divisibilidad por b de cierto número menor de a. (No es difícil ver que la comprobación de la divisibilidad, aplicando la división común, también se basa en esta comprensión.)

De tal modo, el criterio de divisibilidad es un objeto matemático de carácter muy difundido, aunque no salte a la vista. Esto no es *ni* fórmula, ni teorema, ni definición, sino cierto *proceso* absolutamente del mismo tipo como el de la multiplicación «en columna» o, digamos, el de calcular uno tras otro los términos de alguna progresión aritmética.

La noción de criterio de divisibilidad será precisada en el párrafo siguiente.

2. En la definición de la divisibilidad de los números no se dice nada sobre los diferentes valores que puede tener el cociente al dividir a por b. Aclaremos esta cuestión hasta el fin aquí, para que en adelante no tengamos que regresar a ella.

Sea

$$a = bc \qquad (1.1)$$

y, al mismo tiempo,

$$a = bc_1.$$

De estas igualdades obtenemos que

$$bc = bc_1,$$

o que

$$b\,(c - c_1) = 0.$$

Si para este caso $b \neq 0$, entonces $c - c_1 = 0$, o sea, $c = c_1$. Pero si $b = 0$, entonces, evidentemente, también $a = 0$ y la igualdad (1.1) se cumple para cualquier c.

De tal modo, por cero es divisible solamente cero, siendo el cociente de tal división indeterminado. Precisamente se tiene presente esto al hablar sobre la imposibilidad de dividir por cero. Pero si el divisor difiere de cero y la división tiene lugar, entonces el cociente tiene un sólo valor completamente determinado.

Hablando de la división, siempre supondremos que el divisor es distinto de cero.

Fijemos algunas propiedades elementales de la divisibilidad.

TEOREMA 1. $a \vdots a$.

Esta propiedad se llama *reflexiva*.

TEOREMA 2. *Si* $a \vdots b$ *y* $b \vdots c$, entonces $a \vdots c$.

Esta propiedad se llama *transitiva*.

TEOREMA 3. *Si* $a \vdots b$ y $b \vdots a$, *entonces, o bien* $a = b$, *o bien* $a = -b$ (propiedad *asimétrica* de la divisibilidad).

TEOREMA 4. *Si* $a \vdots b$ *y* $|b| > |a|$, *entonces* $a = 0$.

Corolario. Si $a \vdots b$ *y* $a \neq 0$, *entonces* $|a| \geqslant |b|$.

TEOREMA 5. *Para que* $a \vdots b$ *es necesario y suficiente que* $|a| \vdots |b|$.

Basándose en este teorema, basta limitarse en adelante a examinar el caso cuando el divisor es un número positivo. De igual modo, la divisibilidad de números enteros cualesquiera se reduce a la divisibilidad de números no negativos.

TEOREMA 6. *Si* $a_1 \vdots b$, $a_2 \vdots b$, $\ldots$, $a_n \vdots b$, *entonces*,

$$(a_1 + a_2 + \ldots + a_n) \vdots b.$$

Corolario. Si la suma de dos números y uno de los sumandos son divisibles por un número b, entonces, el otro sumando también lo será.

No se debe considerar que todos estos teoremas son evidentes y no han menester de ninguna demostración particular. La cuestión incluso no estriba aquí en que en las matemáticas cualquier afirmación debe ser demostrada, con exclusión del axioma y las definiciones. Las demostraciones de estos hechos (por ejemplo, que cualquier número es divisible por sí mismo) son imprescindibles por principio, dado que ellas no pueden ser obtenidas únicamente de la definición de la divisibilidad sino que se ven en la necesidad de emplear las propiedades de los mismos números.

El siguiente ejemplo nos ayudará a comprender esto más circunstanciadamente.

Evidentemente, la suma, la diferencia y el producto de números pares son siempre pares. Al mismo tiempo, la división de un número par por otro no siempre es factible y, de serlo, el cociente no resulta sin falta par. Por eso introducimos la noción de divisibilidad de números pares.

DEFINICIÓN. El número par a *es divisible de un modo par* por el número par b si existe tal número par c que $a = bc$.

Evidentemente, el teorema 1 no es cierto para la divisibilidad par, dado que, por ejemplo, no existe un número par c tal, que $a = ac$.

A las cuestiones relacionadas con la divisibilidad par de números pares volveremos aún varias veces. El ejemplo anterior muestra que se pueden crear diferentes teorías de divisibilidad con distintas propiedades y que los teoremas, correctos para algunas de estas teorías, pueden resultar incorrectos para otras.

Problemas. Demostrar las siguientes afirmaciones:

1. $0 \vdots a$.

2. $a \vdots 1$.

3. Si $1 \vdots a$, entonces $a = 1$.

4. Cualquiera que sea $a \neq 0$ existe un número b, distinto de a, tal que $b \vdots a$.

5. Cualquiera que sea a, existe un número b tal, que de $b \vdots c$ y $c \vdots a$ se deduce que o bien $c = b$, o bien $c = a$.

6. Demostrar los teoremas análogos a los teoremas 2, 3, 4 y 5 para la divisibilidad par.

7. Construir tal teoría de divisibilidad en la que los teoremas 1, 3 y 4 resulten correctos y los 2 y 6, no.

3. Ya después de tener conocimiento superficial acerca de los hechos concretos de la divisibilidad, salta a la vista la siguiente circunstancia: prácticamente, la divisibilidad de los números no está ligada a su magnitud. Por un lado, hay pequeñas cifras que son divisibles por una cantidad relativamente grande de números. Por ejemplo, 12 es divi-

sible por 1, 2, 3, 4, 6 y 12; 60 tiene 12 divisores. A tales cifras, ricas en divisores, se les pueden oponer números muy grandes con una cantidad mínima de divisores, 2 (de acuerdo al teorema 1 y al problema 2, cada número distinto de la unidad es divisible siquiera por dos números diferentes). Aunque en realidad se conocen algunas leyes que vinculan las propiedades de la divisibilidad de los números con sus valores, de todos modos, ellas tienen un carácter tan intrincado y confuso que aquí no las vamos a tratar.

4. Tanto más interesante resulta el hecho de que la misma divisibilidad permite establecer entre los números un cierto orden, distinto del usual según la magnitud, pero que tiene con el último mucho de común.

En efecto, reflexionamos, qué sentido exacto se expone en las palabras sobre la posibilidad de ordenar los números naturales por sus magnitudes. Como no es difícil ver, bajo esta posibilidad se entiende que para algunas parejas de números a y b tiene lugar la relación «mayor o igual»:

$$a \geqslant b,$$

lo que significa que la diferencia $a - b$ no es negativa (es decir, deberá existir un número natural c tal, que $a = b + c$). ¡Pero si también el fenómeno de la divisibilidad consiste en que ciertas parejas de números a y b responden a alguna condición completamente determinada (precisamente, a la existencia de un entero c, tal que $a = bc$)! Así, las relaciones de divisibilidad y «mayor o igual» son nociones de una misma naturaleza y es por eso que podemos hablar de sus propiedades comunes o, al revés, contraponerlas una a otra.

En particular, la relación de «mayor o igual» entre dos números naturales, lo mismo que la de divisibilidad, es cierta enunciación sobre estos números y puede ser justa (por ejemplo, $5 \geqslant 3$) ó no (por ejemplo, $3 \geqslant 5$).

Señalamos en seguida que con la relación de divisibilidad tiene más propiedades comunes la relación de «mayor o igual» que la de «mayor». Esto está ligado a que la relación de «mayor o igual», semejante a la de divisibilidad, es reflexiva (en efecto, la correlación $a \geqslant a$ es cierta para cualquier a) y la relación de «mayor», no (la desigualdad $a > a$ nunca tiene lugar). Justamente por eso, como relación de orden entre los números naturales, aquí se examina la

de «mayor o igual» y no la «mayor» que parecería más simple y natural.

5. La relación $\geqslant$ tiene las siguientes propiedades, fáciles de comprobar:

1° $a \geqslant a$ (es reflexiva).

2° Si $a \geqslant b$ y $b \geqslant a$, entonces $a = b$ (es asimétrica).

3° Si $a \geqslant b$ y $b \geqslant c$, entonces $a \geqslant c$ (es transitiva).

4° En toda sucesión de números naturales

$$a_1 \geqslant a_2 \geqslant a_3 \geqslant \ldots \geqslant a_n \geqslant \ldots,$$

cuoys términos difieran uno de otro, existirá el número último. Esta propiedad de la relación se llama algunas veces de ordenación u *ordenamiento completo* del conjunto de números naturales.

La propiedad de ordenación completa tiene una formulación bastante complicada y un tanto artificial. No obstante, revela rasgos de extraordinaria importancia en la construcción del conjunto de números naturales ordenados por la relación $\geqslant$. De aquélla se deducen muchas otras propiedades de esta relación. Además, según veremos, precisamente en aquélla están basados los razonamientos «inductivos» tan empleados en distintos problemas matemáticos.

Para el empleo provechoso de esta propiedad señalamos lo siguiente: existe tal número a, que de $a \geqslant b$ se deduce que $a = b$ (aquí a y b son números naturales).

En efecto, si tal número no existiera, entonces, nosotros podríamos encontrar para cada a_n tal a_{n+1} que $a_n \geqslant a_{n+1}$ y $a_n \neq a_{n+1}$. Comenzando con el arbitrario a_1 obtendríamos una sucesión

$$a_1 \geqslant a_2 \geqslant a_3 \geqslant \ldots \geqslant a_n \geqslant a_{n+1} \geqslant \ldots,$$

de nunca acabar. Pero su existencia contraría la propiedad de ordenamiento completo del conjunto de números naturales.

Por consiguiente, el número a señalado realmente existe y se llama *primero* o *mínimo* (evidentemente es el cero). Señalemos aquí mismo que no hemos establecido la unicidad del número mínimo. Lo haremos luego en forma indirecta.

5° Cualquiera que sea el número a existe un número b distinto de a, para el cual $b \geqslant a$.

Esta propiedad del conjunto de los números naturales se llama de *ilimitación*, en el sentido de la relación $\geqslant$.

6° Cualquiera que sea el número a, a excepción de mínimo, existe uno b, que $a \geqslant b$, $a \neq b$ y para cualquier número c, de $a \geqslant c \geqslant b$ se desprende que o bien $c = a$, o bien $c = b$. Esta afirmación formal llevada a un lenguaje substancial significa que cada número natural, a excepción del cero, tiene otro natural inmediato anterior. (Esto también puede ser formulado así: entre todos los números menores que el dado existe uno que es el más grande.)

7° O bien $a \geqslant b$, o bien $b \geqslant a$. Esta propiedad de la relación se llama su *dicotomía*. En matemática, con este término comúnmente se expresa la realización obligada de una de las dos posibilidades. Esta palabra es de origen griego y significa división en dos partes.

Destaquemos que 1°—7° son propiedades de la *propia relación* en el conjunto de todos los números naturales y no las propiedades de unos

u otros números enlazados por esta relación. Por eso puede resultar que para otra relación cualquiera, que una números en parejas no por el valor sino por algún motivo distinto, algunas de las afirmaciones 1°—7° pueden no resultar ciertas.

Problema 8. Basándose únicamente en las propiedades 1°—7° de la relación $\geqslant$ y de ninguna manera en las de los mismos números y las operaciones con ellos:

a) demostrar la unicidad del número mínimo,

b) demostrar la unicidad del número inmediato anterior,

c) formular la definición del número inmediato posterior al número dado a (es decir, del número $a+1$) y demostrar su existencia y unicidad.

Problema 9. Verificar cuáles de las afirmaciones 1°—7° siguen en vigor para la relación de «mayor» ($>$).

6. La justeza de las propiedades de la relación $\geqslant$ (como también, por otra parte, de cualquier otra relación) puede ser establecida de dos maneras. En primer lugar, podemos aprovechar las cualidades de unos u otros números o las particularidades conocidas de la estructura del conjunto de todos los números naturales. Así fueron verificadas por nosotros, precisamente, las propiedades 1°—7°. En segundo lugar, ya convencidos de la justeza de 1°—7°, podemos dejar de lado que la relación $\geqslant$ une números en parejas y deducir las siguientes propiedades de esta relación únicamente de sus propiedades 1°—7°. Así fueron demostradas por nosotros la existencia del número mínimo y las afirmaciones del problema 8.

El segundo enfoque de la cuestión es muy empleado en las matemáticas contemporáneas y lleva el nombre de *axiomático*. Con el se determinan varios *axiomas* (en nuestro caso, las afirmaciones 1°—7°) que reflejan las principales propiedades de los objetos estudiados y no están sujetos a demostración, y de ellos, por medio de la lógica pura, sin recurrir por segunda vez a las propiedades de los objetos estudiados, se deducen todas las restantes afirmaciones llamadas *teoremas*.

Puede ser que a algunos de los lectores el examen de las propiedades de las relaciones sin los objetos enlazados por ellas (por ejemplo, los números) les parezca alcanzar alturas de la abstracción matemática completamente innecesarias en la práctica. Por este motivo es necesario hacer dos observaciones.

En primer lugar, desde el punto de vista de las matemáticas contemporáneas todos los razonamientos efectuados aquí no son en absoluto «particularmente abstractos». Es más, en nuestros días las matemáticas se ven obligadas a examinar simultáneamente muchas relaciones, e incluso unir (!) parejas de relaciones distintas con relaciones nuevas (por decirlo así, de «segundo grado»).

El material expuesto hasta ahora permite ilustrar la noción de relación entre relaciones con un ejemplo.

Sea $\alpha, \beta, \ldots$ un determinado conjunto de relaciones que vinculan números naturales. Esto significa que para cualquier pareja de números a y b y una relación arbitraria γ de nuestro conjunto, sabemos si la pareja a, b está enlazada o no por la relación γ. De estarlo escribiremos $a\gamma b$.

Vamos a decir que la relación α es *más fuerte* que la β, y escribir $\alpha \supset \beta$ si cualquier pareja de números, ligada por la relación β, resulta ligada también por la α, es decir, si de $a\beta b$ sigue $a\alpha b$.

Así, por ejemplo, designando la relación de la divisibilidad par $\vdots$ por medio de p, podemos escribir $\vdots \supset p$. Luego, es evidente que $\geqslant \supset \supset \succ$. Al mismo tiempo, en los conjuntos de números naturales existen relaciones también naturales, con respecto a las cuales no se puede afirmar que una es más fuerte o más débil que otra. Entonces, si para dos números a y b naturales, por ejemplo, suponemos que $a \succ b$ y que la última cifra, en la notación decimal de a, es mayor que la última de b, entonces ni $\succ \supset \geqslant$, ni $\geqslant \supset \succ$.

Claro que para operar libremente con nociones tan complejas como las relaciones entre relaciones es indispensable una práctica especial.

En segundo lugar, tales razonamientos e incluso aún más abstractos se comienzan a encontrar cada vez con más y más frecuencia en las aplicaciones de las matemáticas a la economía, biología, lingüística y al arte militar. Desgraciadamente, explicaciones más detalladas sobre esto nos alejarían demasiado de nuestro tema principal.

7. La posibilidad de emplear el método de *inducción completa* (llamado también de inducción *perfecta* o *matemática*) está estrechamente ligada a la ordenación del conjunto de números naturales por medio de la relación $\geqslant$. Habitualmente este método se emplea de la siguiente manera. Sea $A(n)$ una afirmación concerniente al número natural arbitrario n. Esto significa que, de hecho, operamos con la serie infinita de afirmaciones

$$A(0),\ A(1),\ \ldots,\ A(n),\ \ldots$$

sobre cada uno de los números naturales. Supongamos que

a) la afirmación $A(0)$ es correcta («base de la inducción»)[1];

b) de la corrección de la afirmación $A(n)$ se desprende la de la afirmación $A(n+1)$ («transición inductiva»).

El principio de inducción matemática afirma que en las hipótesis a) y b), $A(n)$ es correcta para cualquier número natural n.

Este principio no es una afirmación independiente, sino que puede ser deducido de las propiedades 1°—7° del conjunto de números naturales ordenados por la relación $\geqslant$.

En efecto, supongamos que las condiciones a) y b) del principio de inducción para la afirmación $A(n)$ se cumplen, pero la conclusión de este principio no tiene lugar. Lo último significa que deben existir tales números m para los cuales la afirmación $A(m)$ no es justa. Sea m_1 uno de ellos. Si para todos los $n < m_1$ la afirmación $A(n)$ es justa, entonces, m_1 es el menor de los números para los cuales $A(n)$ no tiene

[1]) Frecuentemente, como base de una inducción se toma la afirmación $A(1)$. Evidentemente, esta diferencia no es esencial. Lo importante es que dicha base concierne al primero de los números examinados por nosotros.

lugar. Pero si no lo es, entonces deberá existir un $m_2 < m_1$ tal, que $A(m_2)$ sea incierta.

En conclusión, nosotros llegamos a la sucesión de números diferentes

$$m_1 \geqslant m_2 \geqslant \ldots \geqslant m_r \geqslant \ldots, \qquad (1.2)$$

para cada uno de los cuales $A(m)$ no tiene lugar. Por la 4° condición de ordenamiento completo el último término de la sucesión (1.2) deberá ser m_r. Evidentemente, m_r es el menor de todos los números para los cuales $A(n)$ no es cierta.

Por cuanto $A(0)$ es cierta por condición, $m_r \neq 0$, y existe el número m^*, inmediato anterior a m_r (en realidad es el $m_r - 1$). Como $m_r^* < m_r^r$, la afirmación $A(m_r^*)$ deberá ser cierta. Pero entonces, por la condición b) del principio de inducción matemática también lo deberá ser la afirmación $A(m_r^* + 1)$, es decir $A(m_r)$, llegando a una contradicción. Ella indica que no hay números m para los cuales $A(m)$ no tuviera lugar (es decir, no fuera cierta)

Hacemos la siguiente observación. Los razonamientos que acabamos de efectuar no se deben considerar ni demostración, ni fundamento del principio de inducción. Ellos solamente indican que una afirmación matemática (del método de inducción) puede ser deducida de otras (de las propiedades de la relación $\geqslant$). Estas mismas propiedades han sido empleadas por nosotros como axiomas, por lo cual no fueron demostradas sino solamente verificadas. Cualquier intento para demostrarlas en forma matemática tropezaría inevitablemente con la necesidad de introducir condiciones nuevas en calidad de axiomas. En particular, las demostraciones de la propiedad de ordenación completa deberán emplear los mismos razonamientos inductivos (el lector puede cerciorarse de ello por sí mismo).

Al método de inducción matemática en sus diferentes variantes le fueron dedicados los folletos de I. S. Sominski «Método de inducción matemática» (Editorial «Naúka», 1974) y de L. I. Goloviná e I. M. Yaglom «Inducción en la geometría» (Editorial «Naúka», 1956) que contienen gran cantidad de ejemplos de su aplicación. A lo largo de nuestro libro también vamos a emplear este método frecuentemente.

Problema 10. Supongamos que pares de objetos de cualquier naturaleza (números, puntos, funciones, teoremas, etc.) se hallan vincus lados por una determinada relación $\succeq$, con propiedades análogas a la 1°—7°. Demostrar que en este caso estos objetos (elementos) pueden ser numerados (es decir, escritos en un cierto orden): $A_1, A_2, A_3, \ldots$ de modo que $A_i \succeq A_j$, única y exclusivamente cuando $i \geqslant j$.

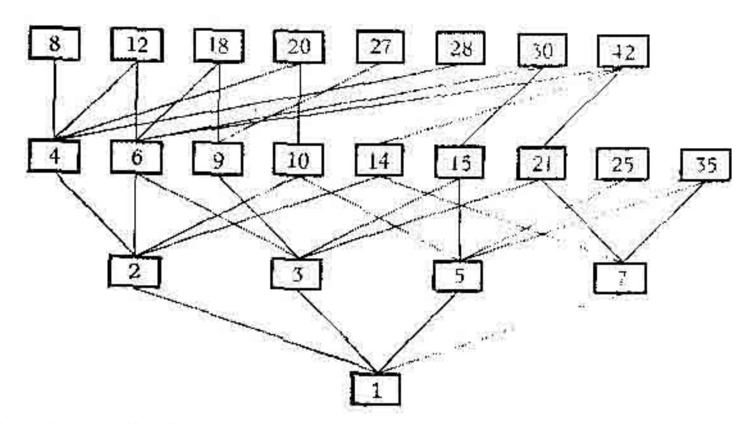
De hecho, lo dicho significa que la relación, poseedora de las propiedades 1°—7°, ordena al conjunto en una cadena lineal de elementos:

$$A_1 \dashv A_2 \dashv A_3 \dashv \ldots$$

8. No obstante, volvamos a la relación de divisibilidad. Para el caso de números positivos los teoremas 1, 2 y 3 y los problemas 3, 4

y 5 muestran que en las afirmaciones 1°—6° podemos sustituir la relación $\geqslant$ por la $\vdots$. En lo que a la afirmación 7° concierne, referida a la aplicación de la divisibilidad, ella afirma: «de dos números uno por lo menos es divisible por el otro».

Pero esto no es cierto. Así, la relación de divisibilidad tiene las mismas propiedades que la de orden, a excepción de una. Debido a esto



la relación de divisibilidad no ordena los números naturales en forma de cadena linear sino de un modo más complejo (véase la figura). Señalamos que los números vecinos por sus valores pueden resultar bastante «alejados» uno de otro en el sentido de la divisibilidad. Los números 4 y 5 ó y 8 lo demuestran claramente

Probemos pasar de la divisibilidad de números enteros positivos a la de naturales, es decir, incluyamos cero en el examen. Entonces el esquema de la figura se enriquece con una casilla ubicada más arriba de las demás, ya que cero es divisible por cualquier número y ninguno distinto de cero es divisible por él.

Dejamos que el lector por su cuenta vuelva a formular y verificar las afirmaciones 1°—7° para este caso.

9. DEFINICIÓN. Cualquier relación $\succeq$, subordinada a las condiciones:

1° de propiedad reflexiva ($a \succeq a$);

2° de propiedad asimétrica (de $a \succeq b$ y $b \succeq a$ se desprende que $a = b$);

3° de propiedad transitiva (de $a \succeq b$ y $b \succeq c$ se desprende que $a \succeq c$), se llama *relación de ordenación parcial*. Las relaciones de ordenación parcial juegan un gran papel allí donde la ordenación lineal «natural» no tiene lugar, por ejemplo, donde cada objeto (se describe o aprecia por varios índices diferentes, cualitativamente incomparables entre sí.

Como ejemplo se puede citar la apreciación de los resultados de las competiciones deportivas para varios tipos diferentes de deportes. Si uno de los equipos ocupó puestos más altos que otro en todos los tipos de programa de competiciones, entonces, es natural considerar que el primer equipo logró mayores éxitos. Pero si estos puestos fueron

ocupados en todos los tipos de programa, a excepción, digamos, del juego de croquet (el cual, por algún motivo, esta vez fue incluido en las competiciones), donde el segundo equipo resultó mejor, entonces, la cuestión sobre la distribución definitiva de los puestos entre nuestros equipos ya no es tan clara. Los entusiastas del croquet pueden exigir, incluso, un puesto más alto para su equipo. De todos modos, cualquier distribución totalizante de puestos estará ligada a determinados recuentos convencionales de los puntos (por ejemplo, al registro de ellos).

10. Las condiciones 1°—3°, cuyo cumplimiento hace que la relación $\succeq$ sea de ordenamiento parcial, son bastante liberales. Por eso con procedimientos muy variados, pueden ser ordenados parcialmente los objetos más distintos, en virtud de lo cual se puede decir bastante poco sobre la relación de ordenación parcial arbitraria, fuera de que ella es de ordenamiento parcial. En particular, a los objetos para los cuales se determinó la relación de ordenación parcial es imposible, hablando es forma general, aplicar el método de inducción matemática.

Completemos, sin embargo, las condiciones 1°—3° con las siguientes:

4° ordenación completa;

5° ilimitación;

6° cada objeto que no sea el mínimo posee un inmediato anterior;

8° cada objeto no tiene más que un número finito de anteriores;

9° cualesquiera que sean a y $b \succeq a$ $(b \neq a)$, existe un c, inmediato anterior de b, tal que $c \succeq a$.

Resulta que a base de la ordenación parcial del conjunto de números naturales con la relación que satisface las condiciones 1°—6°, 8° y 9° se puede construir determinada variante del método de inducción, consistente en lo que sigue.

Sea nuevamente $A\ (n)$ una afirmación concerniente al número arbitrario n. Supongamos que

a) la operación $A\ (a)$ es cierta allí donde, en el sentido de la ordenación $\succeq$, a es el número mínimo;

b) si n es un número y la justeza de cada una de las afirmaciones del tipo $A\ (m)$ ha sido establecida para todos los m, tales que $n \succeq m$ y $n \neq m$, entonces, $A\ (n)$ también es cierta.

La nueva forma del principio de inducción afirma que cumpliéndose las condiciones a) y b), $A\ (n)$ es cierta para cualquier n.

Problema 11. Deducir de la «forma vieja» del principio de inducción una «nueva».

Como la relación de divisibilidad satisface las condiciones 1°—6°, 8° y 9° (formúlense y verifíquense para dicha relación las 8° y 9°), este principio de inducción es aplicable a la relación de divisibilidad.

El nuevo principio de inducción aplicado a la divisibilidad puede ser formulado de tal manera: si una afirmación $A\ (n)$ es correcta para $n = 1$ y de su justeza para todos los divisores de n, distintos de él, se concluye que también para n es cierta, entonces, ella tiene lugar para cualquier número.

11. La división de números enteros, como hemos visto, no siempre se puede hacer. Por eso, paralelamente a la misma, es útil examinar también otra operación más gene-

ral, siempre factible y que, si la división resulta viable, de hecho coincide con ella. Dicha operación es la *división con residuo.*

DEFINICION. *Dividir con residuo* el número a por el b ($b > 0$) significa presentar el primero en la forma

$$a = bq + r,$$

donde $0 \leqslant r < b$.

En este caso, el número q se denomina *cociente incompleto* y el número r, *residuo* de la división de a por b. Está claro que $r = 0$ única y exclusivamente cuando $a \vdots b$. En tal circunstancia q es igual al cociente de dividir a por b.

Mostremos que la división con residuo siempre es factible y que éste y el cociente incompleto quedan enteramente determinados por el dividendo y el divisor, es decir, son únicos.

Sea al principio $a \geqslant 0$. Escribamos los números uno detrás de otro

$$a,\ a - b,\ a - 2b,\ \ldots \qquad (1.3)$$

hasta que aparezca un número negativo (tarde o temprano evidentemente tendrá que aparecer[1])). Aceptemos que el último de los términos no negativos de la sucesión (1.3), es decir, el más pequeño de todos, es el número $a - bq$. Designándolo r tendremos

$$a = bq + r. \qquad (1.4)$$

Indudablemente $r < b$ (de otro modo $r - b$, es decir $a - (q + 1)\,b$, sería no negativo, cosa imposible siendo r *el menor* de los números no negativos de la sucesión (1.3)). De tal modo, (1.4) aparece precisamente como la representación buscada del número a.

Sea ahora $a < 0$. Razonando igual que antes, escribamos la sucesión de los números

$$a,\ a + b,\ a + 2b,\ \ldots$$

hasta que aparezca el primer número no negativo r (es fácil comprobar que $r < b$). Dejemos

$$r = a + bq'.$$

---

[1]) Hablando con más exactitud, esto se desprende de la ordenación completa del conjunto de números naturales por la relación $\geqslant$.

Entonces, designando $-q'$ por q, obtenemos

$$a = bq + r$$

y esto es lo que justamente se pedía.

La posibilidad de división residual fue probada en todos los casos.

Demostremos ahora que esta división es unívoca, es decir, si

$$a = bq + r \tag{1.5}$$

y además

$$a = bq_1 + r_1, \tag{1.6}$$

entonces $q = q_1$ y $r = r_1$.

Tal demostración de la unicidad no se puede simplemente eludir diciendo que, siendo unívoca la operación de sustracción, la sucesión (1.3) puede ser construida por un solo procedimiento; su último término no negativo también es completamente determinado; sea, pues, éste nuestro r . . ., etc. Tal razonamiento aún no nos libra de la posibilidad de obtener otros valores de q y r por cualquiera otra vía absolutamente distinta.

Comparando las relaciones (1.5) y (1.6), nosotros vemos que

$$bq + r = bq_1 + r_1,$$

de donde

$$r - r_1 = b\,(q_1 - q),$$

es decir, $r - r_1$ es divisible por b. Pero $|r - r_1| < b$ y por el teorema 4 esto puede ser solamente cuando $r - r_1 = 0$, o sea, si $r = r_1$. Pero entonces,

$$b\,(q_1 - q) = 0$$

y, considerando que el número b difiere de cero, $q_1 - q = 0$, es decir, $q_1 = q$. Queda probada la unicidad de la división residual.

De tal modo, hemos demostrado el siguiente teorema.

TEOREMA 7 (sobre la división residual). *Para los números arbitrarios a y b ($b > 0$) existen y son únicos tales números r y q, que $a = bq + r$, siendo $0 \leqslant r < b$.*

Hacemos notar que en particular, para $b = 1$, tendremos $r = 0$, de donde $a = q$. Esto responde a la afirmación del

problema 2. Junto con ello queda claro que si $b > 1$, entonces, $a > q$.

Problema 12. Formular y demostrar el teorema de la división residual para la divisibilidad par.

12. DEFINICIÓN. Un número p, distinto de la unidad, se llama *primo* o *simple* si es divisible solamente por sí mismo y por uno.

Primos son, por ejemplo, los números 2, 3, 5, 7, 11, 13, etc.

Un número distinto de la unidad y que no es simple se denomina *compuesto*.

TEOREMA 8. *Los números primos son infinitamente numerosos.*

Cualquier número que divida simultáneamente a los números a y b se llama *divisor común* de estos números. El mayor de los divisores comunes de los números a y b se denomina *máximo común divisor* de ellos y habitualmente se indica por medio de (a, b).

Si el máximo común divisor de a y b es igual a la unidad, entonces se dice que estos números son *primos entre sí*.

Con otras palabras, a y b son primos entre sí si ellos a un tiempo no son divisibles por ningún número, excluyendo la unidad.

TEOREMA 9. *Si a y p son números naturales, siendo p primo, entonces, o bien $a \vdots p$ o bien ambos son primos entre sí.*

Cualquier número divisible simultáneamente por a y b se llama *múltiplo común* de ellos. Al menor múltiplo común positivo de a y b se le denomina *mínimo común múltiplo de* estos números.

TEOREMA 10. *Si M es múltiplo común y m mínimo común múltiplo de a y b, entonces, $M \vdots m$.*

TEOREMA 11. *El mínimo común múltiplo de dos números primos entre sí es igual a su producto.*

* *Corolario.* Para que a sea divisible por los números b y c primos entre sí, es necesario y suficiente que lo sea por el producto de ellos.

TEOREMA 12. *Si $ab \vdots c$, siendo los números b y c primos entre sí, $a \vdots c$.*

TEOREMA 13. *Si el producto de varios factores es divisible por el número primo p, entonces, al menos uno de los factores también es divisible por él.*

Corolario. Si p es primo y $0 < k < p$, entonces el número

$$C_p^k = \frac{1 \cdot 2 \ldots (p-1)\, p}{1 \cdot 2 \ldots (k-1)\, k \cdot 1 \cdot 2 \ldots (p-k-1)(p-k)}$$

es divisible por p.

TEOREMA 14 (Teorema fundamental de la aritmética). *Cualquier número entero positivo, excepto la unidad, puede ser representado en forma de producto de factores primos, siendo el único modo* (los productos que sólo se diferencian por el orden de los factores no se consideran distintos).

El teorema fundamental de la aritmética señala la posibilidad, en principio, de descomponer cualquier número en factores primos. Sin embargo, la realización práctica de tal descomposición presenta tan serias dificultades que las matemáticas contemporáneas todavía, a veces, no pueden superar. En la actualidad los números grandes se descomponen en factores o se establece que son primos por medio de computadoras electrónicas. Así, hace solamente muy poco, se descubrió que el número $2^{19937} - 1$ es primo.

Sea que cierto número a lo tenemos descompuesto en un producto de factores primos. Agrupando los factores iguales obtenemos una fórmula del tipo

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \tag{1.7}$$

donde $p_1, p_2, \ldots, p_r$ son distintos números primos y $\alpha_1, \alpha_2, \ldots, \alpha_r$ varios números enteros positivos. El producto ubicado en el segundo miembro de la fórmula (1.7) se llama *descomposición canónica del número* a.

TEOREMA 15. *Para que los números a y b sean primos entre sí es necesario y suficiente que ninguno de los factores primos que integran la descomposición canónica del número a integre la del número b.*

TEOREMA 16. *Sea* (1.7) *la descomposición canónica del número a. Entonces, para la divisibilidad $b \vdots a$ es necesario y suficiente que*

$$b \vdots p_1^{\alpha_1},\ b \vdots p_2^{\alpha_2},\ \ldots,\ b \vdots p_r^{\alpha_r}.$$

De los teoremas 15 y 16 se desprende que la divisibilidad por el producto de varios números primos entre sí es equivalente a la divisibilidad simultánea por cada uno de ellos.

Problema 13. Estimar desde arriba el mínimo divisor primo del número compuesto a.

TEOREMA 17. *Sea*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

la descomposición canónica del número a. Entonces para la divisibilidad $a \vdots b$ *es necesario y suficiente que la descomposición canónica de b tenga la forma*

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r},$$

donde $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2$, ... $0 \leqslant \beta_r \leqslant \alpha_r$.

Para los fines de este libro resulta muy importante lo siguiente.

TEOREMA 18. *Sean m y t números naturales. Entonces m puede ser presentado como un producto* $m = m_1 m_2$, *donde* $(m_1, t) = 1$ *y se halle tal k para el cual* $t^k \vdots m_2$.

Esto hecho posee analogías algebraicas de largo alcance, que aquí no tocaremos.

Problema 14. Indicar el procedimiento que nos permite construir, por las descomposiciones canónicas de dos números, la descomposición canónica del mínimo común múltiplo de ellos y su máximo común divisor.

Problema 15. Designemos por $\tau(a)$ la cantidad de los distintos divisores del número a (incluidos la unidad y el propio a). Mostrar que para a, cuya descomposición canónica es $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$,

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1).$$

Problema 16. Encontrar a sabiendo que $a \vdots 3$, $a \vdots 4$ y $\tau(a) = 14$.

Problema 17. La descomposición canónica del número a tiene la forma $p_1^{\alpha_1} p_2^{\alpha_2}$ y $\tau(a^2) = 81$. ¿A qué es igual $\tau(a^3)$?

Problema 18. ¿A qué es igual a, si $a = 2\tau(a)$?

Problema 19. Demostrar que es posible hallar un número natural k tal, que para cualquier $K > 0$ y cualquier número a poseedor de k factores primos

$$\frac{\tau(a^2)}{\tau(a)} > K.$$

Problema 20. ¿Son correctos los teoremas análogos a los 11—14 para la divisibilidad par?

§ 2. DIVISIBILIDAD DE SUMAS Y PRODUCTOS

1. Muchas veces en una división residual nos interesa hallar precisamente el residuo de la división del número a por el b, mientras que la magnitud del cociente incompleto de ella no juega ningún papel.

Supongamos, por ejemplo, que queremos saber qué día de la semana será el 1ro de enero del año 2000 (naturalmente, de conservarse hasta esa época el calendario que se emplea hoy). Es fácil enterarse, por el almanaque, que el 1ro de enero de 1980 «cae» en martes. Los veinte años que nos separan de esta fecha están formados por $20 \cdot 365 + 4$ (el último sumando es la cantidad de años bisiestos en el curso de este lapso), o sea, 7305 días, los que componen 1043 semanas completas y 4 días. Al cabo de 1043 semanas será nuevamente martes y, con los cuatro días más, el 1ro de enero del año 2000 va a ser sábado. Evidentemente, para resolver el problema recién planteado no tiene ninguna importancia saber precisamente cuántas semanas completas transcurrieron en 20 años y sólo nos interesa la cantidad de días restantes después de estas semanas.

Con problemas de tal género se encuentran a veces los historiadores, sobre todo los orientalistas, al confrontar las fechas indicadas en distintos calendarios.

Pareciera que para hallar el residuo de la división de un número por otro lo más simple es efectuar directamente la división con residuo. Sin embargo, ella no es tan fácil en la práctica, sobre todo si el dividendo que investigamos no está escrito en el sistema decimal de cálculo a que estamos acostumbrados, sino en forma de expresión compleja del tipo, digamos, $2^{1000} + 3^{1000}$. Al mismo tiempo, la mayor parte del trabajo será invertido en hallar el cociente incompleto que, por sí mismo, no nos es necesario. Por lo tanto se hace indispensable encontrar un procedimiento que nos permita hallar el residuo directamente sin calcular dicho cociente

Presentemos uno de tales procedimientos a base del problema que acabamos de resolver para el 1ro de enero del año 2000. Podemos razonar así. Cada año simple (no bisiesto) se compone de 365 días que forman 52 semanas completas

y un día. El año bisiesto comprende la misma cantidad de semanas y dos días. Quiere decir que todo el lapso desde el 1ro de enero de 1980 al 1ro de enero del año 2000 estará compuesto por un número (no importa cuál) de semanas completas más la cantidad de días igual a la de años transcurridos durante este tiempo, además, cada bisiesto se cuenta por dos. Tal cantidad de días es igual a $20+5=25$. Excluyendo de ella 3 semanas completas resultan 4 días, a contar desde nuestro martes. Ocurre que tal sustitución «año por día» es la manifestación de un recurso muy común cuyo estudio comenzaremos de inmediato.

2. Otro ejemplo, en que el objeto de la división residual es obtener precisamente un residuo, y el cociente incompleto sólo se considera como material de partida para las siguientes operaciones, nos suministra la lista de números en uno u otro *sistema numérico de base* o *posicional*. Recordemos que el número A se denomina número inscripto en el sistema numérico posicional con base t o, mejor dicho, en el t^{nario} sistema numérico (donde t es un número entero positivo, mayor que la unidad), si va presentado en la forma

$$A=a_nt^n+a_{n-1}t^{n-1}+\ldots+a_1t+a_0,$$

donde

$$0\leqslant a_i<t \quad \text{para} \quad i=0,\ 1,\ \ldots,\ n. \qquad (2.1)$$

Los números $a_0, a_1, \ldots, a_n$ se denominan cifras t^{narias} del número A[1]).

Cuando $t=10$ obtenemos un sistema numérico *decimal*. Escribir en este sistema cualquier cifra para nosotros es tan usual, que hablando de un número, habitualmente lo imaginamos sólo de esta forma. En realidad, sin embargo, si las consideraciones corrientes dejan de desempeñar algún papel, como sucede, por ejemplo, al registrar los números en las computadoras electrónicas, también pueden resultar más convenientes otros sistemas de cómputo (el binario, octóneo u octonario, etc.).

Dado que en este libro no hemos de examinar sistemas numéricos que no sean de base (por ejemplo, la notación de

[1]) Una exposición elemental, pero al mismo tiempo profunda, de las cuestiones ligadas a los sistemas de cálculo, se da en el folleto de S. V. Fomin «Sistemas de cálculo» (Ed. «Naúka», 1968).

cifras en números «romanos»), la indicación de que lo son será omitida.

Está claro que de (2.1) resulta

$$A = (a_n t^{n-1} + a_{n-1} t^{n-2} + \ldots + a_1) t + a_0.$$

Es decir, la última cifra t^{aria} del número A es el resto de dividir con residuo A por t. Aquí, el cociente incompleto de tal división se halla entre paréntesis. Dividiéndolo residualmente por t obtenemos

$$(a_n t^{n-2} + a_{n-1} t^{n-3} + \ldots + a_2) t + a_1.$$

La penúltima cifra t^{aria} del número A resulta el residuo. Prosiguiendo este proceso de reiterada división residual por t, conseguiremos sucesivamente todas las t^{arias} cifras del número A, contando de derecha a izquierda (es decir, de inferiores a superiores). Evidentemente (mejor dicho, con arreglo al ordenamiento completo del conjunto de números naturales según la magnitud), este proceso de división residual sucesiva, tarde o temprano ha de interrumpirse. Como resultado lograremos todas las t^{arias} cifras de número A, o sea, su notación en el sistema numérico t^{ario}.

Así, en particular, es como se efectúa el paso de un número de un sistema numérico a otro. Por ejemplo,

$$\begin{aligned} 10\,000 &= 6 \cdot 1666 + 4 \\ 1666 &= 6 \cdot 277 + 4 \\ 277 &= 6 \cdot 46 + 1 \\ 46 &= 6 \cdot 7 + 4 \\ 7 &= 6 \cdot 1 + 1 \\ 1 &= 6 \cdot 0 + 1 \end{aligned}$$

Por eso, 10 000, en el sistema numérico compuesto por 6 guarismos, se escribe como 114144.

3 DEFINICIÓN. Llamaremos *equirresiduales* a los números a y b si, divididos por m, sus residuos o restos resultan iguales.

Fijemos algunas propiedades de tales números.

TEOREMA 19 *Para que los números a y b, al ser divididos por m, sean equirresiduales, es necesario y suficiente que* $(a - b) \vdots m$.

Corolario. Si los números a y b son equirresiduales al dividirlos por m y $m : d$, también lo serán al dividirlos por d.

TEOREMA 20. *Si al dividir por m, los números $a_1, a_2, \ldots, a_n$ son equirresiduales, respectivamente, con los números $b_1, b_2, \ldots, b_n$, entonces, también lo serán los números $a_1 + a_2 + \ldots + a_n$ y $b_1 + b_2 + \ldots + b_n$, así como los $a_1a_2 \ldots a_n$ y $b_1b_2 \ldots b_n$.*

Corolario. Si al dividir por m los números a y b son equirresiduales, entonces también lo serán a^n y b^n para cualquier número natural n.

El teorema 20 y su corolario nos brindan ya posibilidades muy ricas para hallar los residuos de la división. Expongamos algunos ejemplos.

EJEMPLO 1. Hallar el residuo de la división por 3 del número

$$A = 13^{16} - 2^{25}\cdot 5^{15}.$$

Evidentemente, al dividir por 3, 13 resulta equirresidual con 1, 2 con -1 y 5 también con -1. Quiere decir que, a base de lo demostrado, al ser dividido por 3, A es equirresidual con el número

$$1^{16} - (-1)^{25}(-1)^{15} = 1 - 1 = 0,$$

o sea, el residuo buscado es igual a cero y A es divisible por 3.

EJEMPLO 2. Hallar el residuo de la división del mismo número A por 37.

Para esto presentamos A en la siguiente forma:

$$A = (13^2)^8 - (2^5)^5\cdot(5^3)^5.$$

Dado que al ser dividido por 37, $13^2 = 169$ es equirresidual con -16, $2^5 = 32$ con -5 y $5^3 = 125$ con $+14$, entonces el número A íntegro lo es con

$$(-16)^8 - (-5)^5\cdot(+14)^5$$

o, lo que es lo mismo, con

$$(16^2)^4 + 70^5.$$

Pero 16^2, es decir 256, es equirresidual con -3 y 70 con -4. Esto significa que A es equirresidual con

$$(-3)^4 + (-4)^5$$

o, lo que es lo mismo, con

$$81 - (2^5)^2,$$

y, por lo tanto, con

$$81 - (-5)^2 = 81 - 25 = 56.$$

Por fin, 56, al ser dividido por 37, resulta equirresidual con 19, el cual, al no ser negativo y resultar menor de 37, se considera como el residuo buscado.

Problema 21. Hallar el residuo de la división de:

a) $A = (116 + 17^{17})^{21}$ por 8;

b) $A = 14^{256}$ por 17.

Problema 22. Demostrar que para cualquier n:

a) $(n^3 + 11n) \vdots 6$;

b) $(4^n + 15n - 1) \vdots 9$;

c) $(10^{3n} - 1) \vdots 3^{n+2}$;

d) para cualquier a

$$[a^{2n+1} + (a-1)^{n+2}] \vdots (a^2 - a + 1);$$

e) para cualquier k,

$$(n^k - 1) \vdots (n - 1);$$

f) para cualquier k impar,

$$(n^k + 1) \vdots (n + 1).$$

4. Los números a y b que en la división por m son equirresiduales, también se llaman *congruentes respecto al modúlo m*. Esto se indica así

$$a \equiv b \text{ (mód. } m),$$

y la propia fórmula se llama *congruencia*.

La congruencia de dos números respecto a cierto módulo fijo m o, lo que es lo mismo, su propiedad de residuos equivalentes en la división por m, también es una relación que enlaza números enteros entre sí.

Señalemos varias propiedades de la relación de congruencia respecto a un módulo.

1° Propiedad reflexiva: $a \equiv a$ (mód. m).

En efecto, $a - a = 0 \vdots m$.

2° Propiedad simétrica: si $a \equiv b$ (mód. m), entonces $b \equiv a$ (mód. m).

De hecho, si $(a - b) \vdots m$, entonces (aunque sea sólo por el teorema 5), también $(b - a) \vdots m$.

3° Propiedad transitiva: si $a \equiv b$ (mód. m) y $b \equiv c$ (mód. m), entonces, $a \equiv c$ (mód. m).

Para la demostración es suficiente señalar que por el teorema 6, de $(a - b) \vdots m$ y $(b - c) \vdots m$ se deduce que $(a - c) \vdots m$.

Si una relación (la designamos por medio de $\sim$) posee propiedades reflexiva, simétrica y transitiva, se llama *relación de equivalencia* (o

equivalente). El ejemplo más simple de relación equivalente sobre un conjunto de números es la relación de igualdad.

Problema 23. La relación de equivalencia $\sim$ sobre un conjunto de números divide a éste en tales clases o tipos (llamados de equivalencia), que dos números cualesquiera de una misma clase son unidos por la relación de equivalencia y dos cualesquiera de clases diferentes, no. (Demostrarlo).

Este problema trata sobre la relación de equivalencia que enlaza los números. Sin embargo, esto no es sustancial y la afirmación de dicho problema es correcta para relaciones de equivalencia que une objetos de la más arbitraria naturaleza.

Dado que la relación de congruencia respecto al módulo m es relación de equivalencia, también divide un conjunto de números enteros en clases, las cuales se llaman *clases* de restos respecto al módulo m.

4° La cantidad de clases de restos respecto al módulo m es igual a m.

De hecho, dos números a y b pertenecen a una misma clase de restos respecto al módulo m única y exclusivamente cuando al ser divididos por m dan el mismo remanente. Pero el residuo de la división por m puede tener exactamente m valores: $0, 1, 2, \ldots, m-1$. Por consiguiente, también la cantidad de clases es igual a m.

Señalamos una circunstancia extraordinariamente interesante, que hace más preciso el corolario del teorema 19.

Para que cada clase de restos respecto al módulo m_1 esté contenida en alguna clase de restos respecto al módulo m_2 es necesario y suficiente que $m_1 \vdots m_2$.

Efectivamente, examinemos la clase de restos K_1 respecto al módulo m_1 que contiene el número 0. Evidentemente, la clase K_1 esta compuesta, por todos los números que al ser divididos por m_1 dan 0 como residuo es decir, son divisibles por m_1. En particular, ella contiene el número m_1. La clase de restos respecto al módulo m_2 que contiene K_1 también contiene 0 y por eso está compuesta de todos los números divisibles por m_2. Dado que en ella entra el número m_1, deberá ser $m_1 \vdots m_2$. Con esto queda demostrada la necesidad, su suficiencia es evidente.

De tal modo, la relación de divisibilidad puede determinarse por medio de las correlaciones entre las clases de restos. Este procedimiento permite establecer la divisibilidad para objetos de naturaleza mucho más general y compleja que los números naturales. El sucesivo desarrollo de estas ideas conduce a la teoría de grupos, una rama importante del álgebra contemporánea que tiene aplicación en la física teórica y la cristalografía.

Prosigamos la enumeración de las propiedades de la congruencia de los números. Por el teorema 20 se deducen inmediatamente:

5° Si $a \equiv b$ (mód. m) y $c \equiv d$ (mód m), entonces

$$a + c \equiv b + d \ (\text{mód } m).$$

Corolario. Si $a \equiv b$ (mód. m), entonces

$$a + r \equiv b + r \ (\text{mód. } m)$$

para cualquier entero r.

6° Si $a \equiv b$ (mód. m) y $c \equiv d$ (mód. m), entonces

$$ac \equiv bd \text{ (mód } m).$$

Las propiedades 5° y 6° muestran que las congruencias, lo mismo que las igualdades, se pueden sumar y multiplicar por miembros.

Problema 24. Si en un conjunto de números enteros se da la relación de equivalencia $\sim$, que lo divide en m clases, de tal modo que de $a \sim b$ y $c \sim d$ se deduzca $a + c \sim b + d$, entonces, la relación $\sim$ será una congruencia respecto al módulo m (es decir, $a \sim b$ única y exclusivamente cuando $a \equiv b$ (mód. m)).

Problema 25. Formular y demostrar las reglas de simplificación de las congruencias.

Problema 26. Si el número p es primo y a indivisible por él, entonces entre $a, 2a, 3a, \ldots, (p-1)a$ nunca habrá dos números congruentes entre sí respecto al módulo p. Por eso, al dividir los números $a, 2a, 3a, \ldots, (p-1)a$ por p, obtenemos una sola vez cada residuo, a excepción del cero.

Problema 27 (teorema de Wilson). *Para que el número p sea primo es necesario y suficiente que $(p-1)! + 1 = 1 \cdot 2 \ldots (p-1) + 1$ sea divisible por p.*

Problema 28. Formular y demostrar un teorema análogo al 16 para los residuos equivalentes.

§ 3. CRITERIOS DE RESIDUOS EQUIVALENTES Y DIVISIBILIDAD

1. El procedimiento muy general de hallar el residuo de la división de un número a natural arbitrario, aunque fijo, por uno natural dado m, consiste en lo siguiente. Vamos a construir la sucesión de números naturales

$$a = A_0, A_1, A_2, \ldots, \qquad (3.1)$$

equirresiduales para la división por m. El procedimiento de construcción de la sucesión ha de ser tal que a cualquiera de sus términos, mayor o igual a m, lo sucederá por lo menos uno más. Entonces, evidentemente, cualquier término de la sucesión (3.1) menor de m (si desde luego ésta existe), será igual al residuo de la división de a por m. Dicho término puede ser, por ejemplo, el último de la sucesión (asimismo si ella existe).

Uno de los ejemplos más sencillos de tal sucesión es la (1.3), tomada del p. 11, § 1:

$$a, \; a - m, \; a - 2m, \; \ldots$$

De hecho, los problemas de hallazgo de residuo en los ejemplos 1 y 2 del párrafo precedente se reducen a la construcción de sucesiones de este tipo.

Cualquier procedimiento de construcción de la sucesión (3.1) que contenga el último término, será llamado *criterio de residualidad o de residuos equivalentes para la división por m*.

Del ejemplo que acabamos de presentar se desprende que uno de estos criterios es el proceso de ir restando sucesivamente el número m, hasta obtener el primer número menor que él.

2. Evidentemente, para garantizar un criterio seguro de equirresidualidad o de residuos equivalentes es necesario que él satisfaga las tres condiciones siguientes:

1) El criterio de residuos equivalentes debe ser aplicable a cualquier número natural a. Con otras palabras, cualquiera que sea el número a, la sucesión (3.1), construida por él, realmente deberá tener la propiedad antes indicada: después de cada término suyo no inferior a m, deberá seguir siquiera uno más. Esta es la propiedad del criterio, llamada *masividad*.

2) El criterio de equirresidualidad ha de ser preciso en sumo grado. Es decir, el número a debe determinar completamente todos los términos de la sucesión (3.1), sin dejar lugar a ninguna arbitrariedad.

3) Por fin, debemos estar seguros de que al menos un término de la sucesión (3.1) es menor que m. Este requisito podrá ser cumplido si construimos la sucesión (3.1) de tal modo que sin falta posea sólo una cantidad finita de términos, es decir, que el proceso de su construcción no pueda prolongarse un tiempo indefinido, y tarde o temprano termine con la aparición del residuo de la división de a por m. La propiedad del criterio de residuos equivalentes enunciada se llama su *eficiencia*.

3. Los procesos dotados de propiedades de masividad, precisión y eficiencia, se denominan *algoritmos* y en las matemáticas actuales desempeñan un papel cada vez más importante.

Se sobreentiende que la referida caracterización del algoritmo como proceso dotado de las tres propiedades enumeradas, no es su definición exacta. A pesar de haber sido creada por las matemáticas modernas es relativamente

3—01319

compleja y aquí no puede ser formulada. No obstante, los requisitos enumerados reflejan de manera bastante completa las condiciones que deberán satisfacer los procesos matemáticos llamados algoritmos. El papel de estos últimos queda determinado por el hecho de que son procedimientos uniformes de resolución de toda una serie de problemas del mismo tipo. Así, cada criterio de equirresidualidad permite hallar los residuos de la división de un número a variable por uno m fijo.

Hablando algo libremente, se reducen a algoritmos todos los problemas matemáticos cuyas resoluciones pueden ser automatizadas. Por eso, no es casual que el desarrollo de la teoría de los algoritmos coincidió históricamente con la aparición y difusión de las computadoras electrónicas.

A algoritmos se reducen no sólo los problemas de cómputo, en el sentido estricto de la palabra, o sea, aquellos para los cuales, basándose en los datos iniciales, por reglas más o menos complejas se puede obtener una respuesta numérica. También podemos plantearnos la tarea de hallar un algoritmo que nos permita resolver cualquier problema en alguna rama (por supuesto, estrictamente delimitada) de las matemáticas. Este algoritmo deberá ser capaz de transformar las formulaciones de los teoremas en sus demostraciones. A pesar de lo fantástico que nos pueda parecer, tales algoritmos existen, aún cuando se empleen en esferas no muy amplias de las matemáticas. A su vez, en ciertas esferas de éstas (por ejemplo, las que abarcan toda la aritmética), dichos algoritmos no pueden existir en principio.

4. Precisemos, con arreglo a los criterios de residuos equivalentes, el contenido y las consecuencias de observar los tres requisitos planteados a los algoritmos.

De la masividad del criterio de equirresidualidad se desprende que éste deberá transformar diversos números y que los resultados de tales transformaciones, hablando en general, también deberán ser distintos (ya que al dividir por cualquier $m > 1$, no todos los números redundan equirresiduales entre sí). Esto significa que como parte integrante includible de este proceso tiene que figurar la distinción (por sus magnitudes) de los números.

La propiedad de precisión del criterio de equirresidualidad significa que los números ya anotados $A_0, A_1, \ldots, A_n$ de la sucesión (3.1) deben ser «identificables» a tal punto

que a base de ellos se pueda escribir el número siguiente de dicha sucesión, A_{n+1}.

Por fin, la propiedad de eficiencia, además de todo eso, también lleva tras de sí una necesidad de posibilidades ilimitadas para comparar (por la magnitud), en cada paso de nuestro proceso, el número obtenido A_k con el divisor m.

Así pues, la observancia de cada uno de los tres requisitos algorítmicos por el criterio de equirresidualidad se apoya, ante todo, en la indefectible necesidad de poder comparar (por sus magnitudes) los números que se hallan entre los pares arbitrarios, e indicar, en el caso de que lleguen a ser distintos, cuál de ellos es mayor y cuál menor.

5. La «necesidad de poder comparar», mencionada hace un momento, también es, evidentemente, de naturaleza algorítmica: dos números naturales cualesquiera estarán sujetos a ser comparados (masividad) y su resultado ha de ser una sóla respuesta: mayor, menor o igual (precisión) y ella será obtenida siempre (eficiencia). Quiere decir que esto nos da facultad para hablar de algoritmos de comparación (por la magnitud) de dos números. Su construcción no es algo muy evidente, como podría parecerlo a primera vista. Por ejemplo, resolver el problema de si los números

$$2^{20} - 3\cdot5^2\cdot11\cdot31\cdot41 \quad \text{y} \quad 3^{10} - 2\cdot3\cdot13\cdot757 \qquad (3.2)$$

son iguales o diferentes y, en el último caso, cuál de ellos es el mayor, requiere consabidos esfuerzos, aunque en realidad, el primero de estos números es solamente uno, y el segundo 3.

Es evidente que la comparación de los números de (3.2), según su magnitud, es difícil debido a la forma de su escritura. Por lo tanto, para construir los criterios de equirresidualidad es muy importante presentar los números de tal manera que, infaliblemente, puedan ser comparados con arreglo a su magnitud. Dichas formas de escritura existen.

Por ejemplo, son las que se hacen en unos u otros sistemas numéricos (de base) (véase § 2 p. 2). El algoritmo para comparar dos números, escritos en un mismo sistema numérico, estriba en lo que sigue:

1) Al principio en cada número se tachan las cifras una por una (comenzando, digamos, desde la derecha); si, después que uno de ellos resulta completamente tachado, al otro aún le quedan guarismos, entonces el segundo será mayor

que el primero; pero si en ambos números las reservas de cifras fueron agotadas al mismo tiempo, entonces, para compararlos se ejecuta el siguiente procedimiento:

2) Las inscripciones de los números que se verifican se restablecen comparando sus primeros (desde la izquierda) guarismos. En este caso, cuanto mayor sea la cifra, mayor será el número; si las cifras resultan iguales, entonces pasamos a comparar las segundas, etc., hasta que aparezca la primera diferencia de éstas. Además, cuanto mayor sea el guarismo, mayor será el número. Si todas las cifras respectivas de los números resultan idénticas, todos los números serán iguales.

Al efectuar el segundo de los procedimientos indicados, se supone que sabemos cómo comparar la magnitud de los números unívocos, o sea, menores que la base del sistema numérico. Esto significa que en cada sistema numérico los signos-cifras iniciales de antemano son presentados en cierto orden fijado; por ejemplo, en la numeración decimal corriente, el signo «2» antecede al «3», en el sentido de que el primero describe una cantidad menor que el segundo.

Desde el punto de vista de tal cotejo algorítmico, todos los sistemas numéricos son equivalentes teóricamente. En este sentido, la comparación misma de los sistemas numéricos puede servir, según su comodidad práctica, de ejemplo de planteamiento no algorítmico de la cuestión (no se cumple la condición de precisión), pero en ésta no nos detendremos. Sólo prestemos atención al hecho de que en dicha cuestión la fuerza de la costumbre de trabajar con el sistema de números decimales no nos brinda ninguna ventaja particular.

6. Además de los algoritmos de comparación de números, escritos en un mismo sistema numérico, existen también aquellos con los que se ejecutan operaciones aritméticas. Son los procedimientos de adición, sustracción y multiplicación de números «en columna» y la división «sexagesimal» de ellos, universalmente conocidos (y que, evidentemente, dependen poco de la base del sistema numérico). Claro está que en el último procedimiento lo más adecuado quizás sería no hablar simplemente de división, sino de división residual.

Al ejecutar las operaciones, nos proporciona un gran alivio la práctica de manejo del sistema de números decima-

les. Por ejemplo, la ejecución de la operación

```
     13110 |224
     1232  |‾‾31
    ─────
       240
       224
    ─────
        11
```

en el sistema quinario de numeración requiere determinados esfuerzos mentales.

De la algoritmización de la división residual se desprende también, según lo dicho en el p. 2 § 2, la algoritmización del paso de la escritura de los números de un sistema de numeración a otro. Por consiguiente, podemos hablar también de los algoritmos de comparación de números y de ejecución de operaciones con ellos, si es que se hallan escritos en distintos sistemas numéricos. Como deducción ulterior, de aquí resulta que todas las clases de cómputos, utilizando fórmulas aritméticas en las que en lugar de letras podamos colocar unos u otros números, son algoritmos.

Y, por fin, prestemos atención al hecho de que aquí no hablamos del algoritmo del propio proceso de escritura de los números naturales, arbitrariamente presentados en uno u otro sistema numérico, ya que nadie sabe cuál puede ser el problema inicial.

7. Como ejemplo ilustrador examinemos la siguiente construcción. Componemos para cada número natural n la sucesión de número (cifras) $a_0^{(n)}, a_1^{(n)}, a_1^{(n)}, \ldots$, que son las cifras de una descomposición decimal infinita del número $\sqrt{n}$ (si el número n no es exáctamente un cadrado, evidentemente, esta sucesión resulta aperiódica), admitiendo que $r_1^{(n)}, r_2^{(n)}, \ldots$ son los números de las cifras iguales a cero: $a_{r_i^{(n)}}(n) = 0$ $(i = 1, 2, \ldots)$. Si ahora la cantidad de guarismos iguales a cero es finita (con el último de ellos, un número $r_h^{(n)}$ tal, que $a_i^{(n)} > 0$ para $i > r_h^{(n)}$,) ponemos que

$$f(n) = 10^{r_1^{(n)}} + 10^{r_2^{(n)}} + \ldots + 10^{r_h^{(n)}} + 1,$$

pero si la cantidad de ellos es infinita, entonces admitiremos, digamos, que $f(n) = 0$. Cada uno de los números $f(n)$ es natural. Con todo se torna dudoso hablar de un algoritmo capaz de transformar el número n en la escritura del número $f(n)$, dentro del sistema numérico decimal.

Se sobreentiende que la no algoritmosidad de esta construcción consiste en la exigencia de discernir si en la descomposición decimal $\sqrt{n}$ resultará un número finito o infinito de ceros. A propósito, en cierto sentido (precisamente en cuál, no hemos aquí de tratar), *es natural pensar* que para cualquier número natural n, $f(n) = 0$.

8. Uno de los más importantes algoritmos en las matemáticas, que lleva el nombre de Euclides, radica en lo siguiente.

Sean a y b dos números naturales y además $b > 0$. Realicemos la división residual de a por b: $a = bq_0 + r_1$, donde $0 \leqslant r_1 < b$. Si $r_1 \neq 0$, podemos realizar la división residual de b por r_1: $b = r_1q_1 + r_2$, donde $0 \leqslant r_2 < r_1$. Prosiguiendo estas sucesivas divisiones residuales por el residuo de la división precedente obtenemos las siguientes igualdades: $r_1 = r_2q_2 + r_3$, $r_2 = r_3q_3 + r_4$, etc.

Mostremos que el proceso descripto es verdaderamente un algoritmo, es decir, que posee las propiedades de precisión, masa y eficiencia.

Señalamos que el proceso examinado por nosotros radica en efectuar sucesivas divisiones residuales.

Por eso, las propiedades de precisión y masa de este proceso son resultados de la ilimitada posibilidad de realización y unicidad de la división residual. La eficiencia de nuestro proceso se determina también muy fácilmente. El número b y los residuos de las divisiones integrantes de nuestro proceso forman, evidentemente, sucesiones decrecientes de números no negativos

$$b, r_1, r_2, \ldots \tag{10}$$

Pero la cantidad de todos los números no negativos, no mayores de b, es igual a $b + 1$. Por eso, tampoco la sucesión (10) puede contar con más de b términos. Así, nuestro proceso no podrá estar formado por más de b divisiones residuales[1]). De tal manera, el proceso examinado es, efectivamente, un algoritmo y justifica con toda plenitud su denominación.

Aclaremos las condiciones en que finaliza el proceso. Evidentemente, la última división deberá ser tal que haga imposible seguir dividiendo por su residuo. Pero esto ocurre solamente cuando él es igual a cero, o sea, cuando la última división resulta exacta.

Problema 29. a) El último residuo r_n diferente de cero, en la aplicación del algoritmo de Euclides a los números a y b es (a, b).

b) Cualesquiera que sean los naturales a y b, existen tales enteros A y B que $aA + bB = (a, b)$.

Problema 30. Deducir los teoremas 9, 12, 13 y 14 del resultado b) del problema 29. (Subrayamos que nuestros razonamientos, ligados al algoritmo de Euclides, fueron basados solamente en la posibilidad de efectuar divisiones residuales. Nosotros no empleamos en ellos ni los teoremas 9—14 ni cualesquiera otras consideraciones basadas en el teorema fundamental de la aritmética.)

9. La aplicación de los algoritmos (por decirlo así, «su trabajo») puede resultar bastante voluminosa. Examinemos, como ejemplo, el proceso para obtener su descomposición canónica por el número n (o sea, el algoritmo que trans-

[1]) De hecho, el número de estas divisiones no tiene que sobrepasar 5 log b, lo cual se desprende al examinar los números de Fibonacci (véase, por ejemplo, el libro del autor «Números de Fibonacci», Editorial «Naúka», 1978, págs. 82—83).

forma un número natural en su descomposición canónica). Para destacar la esencia algorítmica de este proceso incluyámoslo, como etapa, dentro del proceso de hallazgo sucesivo de las descomposiciones canónicas de todos los números naturales, uno tras otro. Esto avala los siguientes razonamientos hechos «por inducción» (véase p. 7, § 1). Supongamos que para todos los números menores de n, las descomposiciones canónicas ya han sido escritas. Por tal lista es posible saber (en forma completamente algorítmica) cuáles de los números inferiores a n son primos. Enumerándolos de menor a mayor, cada uno de ellos será dividido por n. Si n es divisible por cierto p, entonces $n = n_1 p$ y $n_1 < n$, pero la descomposición canónica de n, por lo supuesto, figura en nuestra lista (visto el resultado del problema 13 es suficiente dividir sólo por aquellos p que son menores de $\sqrt{n}$) y se obtiene la descomposición canónica por la descomposición canónica de n_1, aumentado en ella el exponente p en la unidad.

10. Volvamos, no obstante, a los criterios de equirresidualidad. La construcción algorítmica de la sucesión (3.1) puede ser efectuada por muy diversas vías. La más natural es la siguiente.

Procuremos hallar la función $f(x)$ sujeta a las condiciones que siguen:

a) para $x \geqslant m$ el valor de $f(x)$ es un número natural;

b) para $x < m$ el valor de $f(x)$ es indeterminado (es decir, no tiene sentido);

(no es nada asombroso que una u otra función pierda su sentido para ciertos valores del argumento. Por ejemplo, no lo tiene el valor de la función $\frac{1}{x(x-1)}$ para $x = 0$ o $x = 1$);

c) si $x \geqslant m$, entonces $f(x) < x$;

d) si $x \geqslant m$, entonces los números x y $f(x)$ son equirresiduales para la división por m.

Tales funciones existen. Por ejemplo, $f_0(x)$:

$$f_0(x) = \begin{cases} x - m, & \text{para } x \geqslant m, \\ \text{indeterminada}, & \text{para } x < m. \end{cases}$$

Justamente, ésta es la función con la que se construye la sucesión (1.3) en § 1.

Cada función $f(x)$ que satisfaga las condiciones a)—d)

responde a cierto procedimiento de construcción de la sucesión (3.1), es decir, a determinado criterio de residuos equivalentes para la división por m.

Efectivamente, tomemos el número natural arbitrario a y construyamos la sucesión de números

$$A_0, A_1, A_2, \ldots, \qquad (3.4)$$

donde $A_0 = a$ y $A_{k+1} = f(A_k)$ para $k = 0, 1, \ldots$ (3.5)

Si $A_k \geqslant m$, el valor de la función $f(A_k)$ es determinado, por lo que a A_k le sigue al menos un término más. Pero si $A_k < m$, $f(A_k)$ es indeterminado y A_k resulta el último término de la sucesión (9).

Así, nosotros tenemos verdaderamente cierto criterio de residuos equivalentes.

11. Mostremos que el criterio de equirresidualidad hallado posee las tres propiedades del algoritmo.

La condición de masividad aquí es observada, ya que cualquier número da comienzo a cierta sucesión (3.4) dotada de la propiedad (3.5).

La condición de precisión se ve cumplida, dado que para calcular los valores de $f(x)$ de la función f es suficiente saber comparar por la magnitud los números x y m y efectuar la operación de sustracción (restando m de x). Como fue explicado, ambos procedimientos (de tratarse de números escritos en cierto sistema numérico) son algoritmos y por lo tanto poseen propiedad de precisión.

Dirijámonos a la condición de eficiencia. La función fue elegida tal que, por su propia construcción, los términos de la sucesión (3.4) son positivos y decrecientes. Por eso en ella podemos encontrar el término mínimo no negativo. (Su número, como es fácil de comprobar, no supera al número a). Pero si este término (llamémoslo α) fuera mayor o siquiera igual a m, entonces existiría, como antes, un valor de $f(\alpha)$ no negativo, pero menor de α. Esto significaría que entre los términos no negativos de la sucesión (3.4), α no sería el último. Por consiguiente, el último término no negativo de (3.4) deberá ser *menor* que m. Pero entonces el valor de $f(\alpha)$ pierde todo sentido y, hablando en general, α resulta el último término de nuestra sucesión. De tal modo, el proceso de construcción de la sucesión concluye y su último término es el residuo de la división de a por m.

En conclusión, hemos constatado que el criterio de residuos equivalentes, descripto por nosotros, verdaderamente posee las propiedades de precisión, masividad y eficiencia requeridas, o sea, es un algoritmo.

12. Empleando el procedimiento expuesto en el p. 9 para formar los criterios de equirresidualidad, hallemos algunos de ellos. Coincidiendo con lo dicho anteriormente, consideraremos que los números cuyos residuos de su división es preciso hallar, están escritos en un sistema posicional numérico de cierta base t. El criterio de equirresidualidad para la división por cierto m, al dividir por dicho m, transforma, de hecho, en residuo no el propio número, sino a su escritura, en concordancia con el sistema numérico. Por eso, hablando en general, el criterio de residuos equivalentes para la división por un número concreto fijo, dependerá de la base del sistema numérico. Simultáneamente, la formulación textual del criterio de equirresidualidad para la división por un m dado, en un t^{uario} sistema de numeración, puede valer plenamente para el criterio de equirresidualidad al dividir por otro m' en un sistema numérico con otra base t'. Los ejemplos respectivos serán tomados del contenido de los teoremas 19, 20 y 21.

Para evitar posibles malentendidos convengamos que, en adelante, vamos a escribir («denominar») tanto el divisor m, como la base t del sistema numérico, en el sistema de numeración decimal. Así, al hablar del criterio de residuos equivalentes para la división por 12 en el sistema septenario de numeración, hemos de entender que 12 precisamente es el número $3 \cdot 4$ y no el $3 \cdot 3$ (así resultaría si 12 fuera examinado como un número escrito en el sistema septenario de numeración).

Como primer ejemplo hallemos el criterio de residuos equivalentes para la división por 5 en el sistema decimal de numeración.

Sea A un número natural. Presentémoslo con la forma $10\,a + b$ (b es la última cifra del número A) y admitamos que

$$f_1(A) = \begin{cases} b, & \text{si } A \geqslant 10, \\ b-5, & \text{si } 5 \leqslant A < 10, \\ \text{indeterminada}, & \text{si } A < 5. \end{cases}$$

El lector puede verificar por sí mismo que una función determinada de este modo satisface las condiciones a)—d) del p. 10.

De tal modo, para hallar el residuo de la división de cierto número por 5 es suficiente tomar su última cifra. Si ella es menor que 5, entonces, precisamente, será el residuo buscado; en caso contrario debemos quitarle 5. Señalamos que para cualquier número el empleo de este criterio de residuos equivalentes conduce a construir una sucesión del tipo (3.4), compuesta por no más de tres términos.

Desde luego, el objeto de todos los razonamientos efectuados no es descubrir «el criterio de divisibilidad» por 5 que conocemos todos, sino obtenerlo por el procedimiento uniforme descripto en el p. 10.

Problema 31. Señalar y analizar los criterios análogos de residuos equivalentes para la división por 2, 4, 8, 10, 16, 20 y 25 en el sistema decimal de numeración.

Problema 32. Señalar y analizar los criterios análogos de equirresidualidad para las divisiones por:

a) 9 y 27 en el sistema ternario de numeración;

b) 8, 9, 16, 18, 24, 36, 48 y 72 en el sistema duodecimal de numeración.

Problema 33. Presentemos el número natural A en la forma

$$10^k a + b \quad (0 \leqslant b < 10^k)$$

y admitamos que

$$f(A) = \begin{cases} b, & \text{si } A \geqslant 10^k, \\ \text{al residuo de la división de } A \text{ por } m, & \text{si } m \leqslant A < 10^k, \\ \text{indeterminada}, & \text{si } A < m. \end{cases}$$

¿Cuáles son los números m con los que tal algoritmo, para cierto k, es criterio de residuos equivalentes?

TEOREMA 21 *Presentemos el número arbitrario natural A en la forma $at^k + b$, donde $0 \leqslant b < t^k$, y pongamos que*

$$f(A) = \begin{cases} b, & si\ A \geqslant t^k, \\ b - m, & si\ m \leqslant A < t^k, \\ indeterminada, & si\ A < m. \end{cases}$$

A fin de que el algoritmo de construcción de la sucesión (3.4) por la regla (3.5) sea criterio de equirresidualidad para la división por m con una función dada f, es necesario y suficiente que $t^k \vdots m$.

13. Como segundo ejemplo examinemos el criterio de residuos equivalentes para la división por 3 en el sistema decimal de numeración.

La escritura del número natural A en el sistema decimal de numeración tiene la forma

$$a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 \cdot 10 + a_0,$$

donde

$$0 \leqslant a_i < 10 \quad \text{para} \quad i = 0, 1, \ldots, n.$$

Admitamos que

$$f_2(A) = \begin{cases} a_0 + a_1 + \ldots + a_{n-1} + a_n, & \text{si } A \geqslant 10, \\ \text{al residuo de dividir } A \text{ por } 3, & \text{si } 3 \leqslant A < 10, \\ \text{indeterminada}, & \text{si } A < 3. \end{cases}$$

Problema 34. Verificar que la función $f_2(x)$ satisface las condiciones a)—d) y determina con ello un criterio de residuos equivalentes en la división por 3.

Problema 35. Aplicar el criterio construido de residuos equivalentes para la división por 3:

a) a los números 858 773 y 789 988;

b) al número, cuya notación decimal está compuesta de 4444 cuatros.

Problema 36. Señalar y analizar los criterios análogos de residuos equivalentes para la división por 7, 9, 11, 13 y 37 en el sistema decimal de numeración.

Problema 37. Señalar y analizar los criterios de equirresidualidad para la división por:

a) 2, 4 y 8 en el sistema de numeración ternario;

b) 2, 4 y 8 en el sistema de numeración septenario.

TEOREMA 22. *Presentemos el número arbitrario natural A en la forma*

$$a_n t^{kn} + a_{n-1} t^{k(n-1)} + \ldots + a_1 t^k + a_0,$$

donde

$$0 \leqslant a_i < t^k \quad \text{para} \quad i = 0, 1, \ldots, n,$$

y admitamos que

$$f(A)=\begin{cases} a_0+a_1+\ldots+a_{n-1}+a_n, & \text{si } A\geqslant t^h,\\ A-m, & \text{si } m\leqslant A<t^h,\\ \textit{indeterminada}, & \text{si } A<m. \end{cases}$$

Entonces, para que el algoritmo engendrado por la función f de construcción de la sucesión (3.4), por la regla (3.5), sea criterio de equirresidualidad para la división por m, es necesario y suficiente que $(t^h-1):m$.

Problema 38. Indicar los criterios de residuos equivalentes que «caen» bajo la férula de este teorema para los números escritos en los sistemas numéricos de base 7; 9 y 13 o compuestos de 6, 7, 9 y 13 guarismos.

TEOREMA 23. *Sea A un número natural presentado en la forma*

$$a_nt^{hn}+a_{n-1}t^{h(n-1)}+\ldots+a_1t^h+a_0,$$

donde

$$0\leqslant a_i<t^h \quad \textit{para} \quad i=0,\ 1,\ \ldots,\ n.$$

Admitamos que

$$f(A)=\begin{cases} a_0-a_1+a_2-\ldots\pm a_n, & \text{si } A\geqslant t^h,\\ \textit{al residuo de dividir } A \textit{ por } m, & \text{si } m\leqslant A<t^h,\\ \textit{indeterminada}, & \text{si } A<m. \end{cases}$$

Entonces, para que el algoritmo de construcción de la sucesión (3.4) por la regla (3.5), engendrado por la función f, sea criterio de equirresidualidad para la división por m, es necesario y suficiente que $(t^h+1):m$.

Problema 39. Señalar el criterio de equirresidualidad que «cae» bajo la férula de este teorema, para los números escritos en los sistemas numéricos ternario, quinario, octonco u octonario y decimal.

14. En muchos problemas tiene poca importancia no sólo la magnitud del cociente incompleto de la división de un número por otro, sino también, la de su residuo, y únicamente interesa el hecho de que este último se anula o no, es decir, sea o no el primer número divisible por el segundo. Después de lo dicho en el p. 1 queda claro cómo enfocar los problemas de tal tipo.

Llamaremos *equidivisibles* en la división por m a los números a y b si ambos son divisibles por m o si ambos no lo son.

Problema 40. Cualesquiera que sean los números de residuos equivalentes para la división por m, fuera cual fuese este último, son equidivisibles por él. Mostrar en un ejemplo que lo inverso no es cierto.

Problema 41. ¿Para cuáles m que dividan dos números, de la equidivisibilidad de éstos se deducen sus equirresidualidades en tal división?

Problema 42. Demostrar que la relación de equidivisibilidad, para la división por un número dado m, es equivalente y divide el conjunto de números enteros en dos clases.

Problema 43. ¿Son correctos el teorema 20 y su corolario para los números equidivisibles?

15. Admitamos la necesidad de poner en claro la divisibilidad de A por m. Vamos a construir la sucesión de números enteros decrecientes:

$$A = A_0, A_1, A_2, \ldots, \tag{3.6}$$

equidivisibles con A para la división residual por m. Elegimos un proceso de construcción de la sucesión (3.6) tal, que a cualquier término de ella, mayor o igual en valor absoluto a m, le suceda por lo menos uno más. Así, cuando el último término de (3.6) es igual a cero, A es divisible por m y cuando no, no lo es.

Cualquier procedimiento de construcción de la sucesión (3.6) será llamado *criterio de divisibilidad por m*.

Problema 44. Demostrar que cualquier criterio de residuos equivalentes para la división por m es criterio de divisibilidad por m.

Evidentemente, los criterios de divisibilidad tienen que ser algoritmos, es decir, satisfacer las mismas condiciones de precisión, masividad y eficiencia que los criterios de equirresidualidad.

Es fácil comprobar (se lo dejamos al lector) que empleando cualquier función $f(x)$, que satisfaga las condiciones a)—c) del p. 10 y la condición d*), si $f(x)$ tiene sentido, los números x y $f(x)$ son equidivisibles por m, se puede construir el criterio de divisibilidad por m exactamente del mismo modo como se construyó el criterio de residuos equivalentes para la división por m a base de toda función que satisfaga las condiciones a)—d).

Hallemos algunos criterios de divisibilidad.

Según el teorema 16 es suficiente poder determinar la divisibilidad de los números por uno del tipo p^α (elevado a la potencia de un número primo).

16. Criterio de divisibilidad por 7 en el sistema decimal de numeración. Sea A un número natural. Presentémoslo, como ya se hizo anteriormente, en la forma $10a + b$, donde $0 \leqslant b < 10$, admitiendo que

$$f_3(A) = \begin{cases} |a-2b|, & \text{si } A \geqslant 19, \\ \text{al residuo de la división de } A \text{ por } 7, & \text{para } 7 \leqslant A < 19, \\ \text{indeterminada,} & \text{para } A < 7. \end{cases}$$

Problema 45. Verificar el cumplimiento de las condiciones a)—c) y d*) para la función $f_3(A)$.

La función $f_3(A)$ nos da un criterio conocido de divisibilidad por 7: el guarismo $10a + b$ $(0 \leqslant b < 10)$ es divisible por 7, única y exclusivamente cuando lo es $a - 2b$; el número obtenido se verifica nuevamente a la divisibilidad por 7 con este procedimiento, etc.

Problema 46. Demostrar que el criterio obtenido de divisibilidad por 7 no es el criterio de residuos equivalentes para la división residual por 7.

17. Criterio de divisibilidad por 13. Presentemos el número natural A en la forma $10a + b$, admitiendo que

$$f_4(A) = \begin{cases} a+4b, & \text{si } A \geqslant 40, \\ \text{al residuo de la división de } A \text{ por } 13, & \text{si } 13 \leqslant A < 40, \\ \text{indeterminada,} & \text{si } A < 13. \end{cases}$$

Problema 47. Verificar el cumplimiento de las condiciones a)—c) y d*) para la función $f_4(x)$ y formular el criterio obtenido de divisibilidad por 13.

Problema 48. ¿Qué efectos tendrá la sustitución del número 40 por uno menor en la determinación de la función f_4?

Problema 49. En forma similar a las construcciones de los criterios de divisibilidad por 7 y 13 componer los criterios análogos de divisibilidad por 17, 19, 23, 29 y 31.

Problema 50. Construir dos criterios de divisibilidad por 49.

18. También para los números escritos en otros sistemas de numeración, no decimales, hay criterios de divisibilidad de ese mismo tipo.

¿El criterio de divisibilidad por 11 en el sistema de numeración de base 6 o compuesto de 6 guarismos. Presentemos el número natural A en la forma $6a + b$, donde $0 \leqslant \leqslant b < 6$ (en concordancia con lo anteriormente dicho, todos los razonamientos se efectúan empleando los signos y denominaciones de los números en el sistema decimal de numeración) y pongamos que

$$f(A) = \begin{cases} a + 2b, & \text{si } A \geqslant 11, \\ 0, & \text{si } A = 11, \\ \text{indeterminada}, & \text{si } A < 11. \end{cases}$$

Problema 51. Verificar el cumplimiento de las condiciones a)—c) y d*) para la función f y formular el criterio de divisibilidad obtenido.

Problema 52. Análogo al criterio de divisibilidad acabado de construir, construyamos los criterios de divisibilidad por:

a) 5, en el sistema de numeración septenario;

b) 7, en el sistema de numeración de base 11 o compuesto de 11 guarismos;

c) 17, en el sistema de numeración duodecimal.

19. En los puntos anteriores de este párrafo nosotros hemos visto gran cantidad de los más diferentes criterios de residuos equivalentes y divisibilidad. La finalidad práctica de la construcción de todos estos criterios es obtener algoritmos fácilmente manejables que determinen los residuos en la división por algunos números determinados (criterios de residuos equivalentes) o nos revelen si tales residuos son iguales a cero o no (criterios de divisibilidad). ¿Hasta qué punto hemos cumplido, pues, el objetivo propuesto?

Algunos criterios de equirresidualidad, tales como los de la división por 2, 3, 5 y 10 en el sistema decimal de numeración (y en general, por el divisor del grado de la base del sistema de numeración), realmente resultaron muy

prácticos y convenientes. El empleo de otros está ligado a operaciones de cálculo más o menos voluminosas.

Es natural, entonces, buscar y aplicar los criterios de divisibilidad y residuos equivalentes, cuyo empleo lleva al objetivo por las vías más sencillas posibles.

Una de las dificultades con las que se tropieza en tal tipo de pruebas es valuar la sencillez (o al revés, la complejidad) del empleo de tal o cual criterio con un número. Tal característica numérica puede ser, por ejemplo, la cantidad de operaciones aritméticas con números dígitos necesarias durante el proceso de aplicación del criterio dado a uno u otro número.

Por desgracia, toda característica del volumen de los cálculos depende en gran medida de las propiedades individuales del número cuya divisibilidad ensayamos.

Por ejemplo, podemos comprobar con mucha facilidad que el residuo de la división de 31 025 por 8 es 1. Para ello basta con hallar el residuo de la división de 25 por 8. Pero para hallar el de la división de 30 525 por 8 hay que realizar la división residual de 525 por este último, lo cual ya requiere un mayor número de cómputos (siendo indistinto que se efectúen mentalmente o por escrito).

Otro ejemplo es el criterio de residuos equivalentes para la división por 37 (véase el problema 36). El residuo de dividir 10 014 023 por 37 se halla dividiendo por él la suma $10 + 14 + 23$. Como es fácil de ver, resulta igual a 10. De todos modos, pocos son los que pueden aplicar mentalmente este criterio de residuos equivalentes al número 782 639 485.

Por eso, al tratar sobre la conveniencia del empleo de los criterios de divisibilidad y residuos equivalentes, nosotros tenemos que dejar de lado la complejidad de las pruebas individuales de divisibilidad de los números y valorar las posibilidades de cada criterio como «término medio». Con tal enfoque es de esperar una formulación precisa de la medida de complejidad del criterio de divisibilidad o de residuos equivalentes o incluso hallar el que en este sentido sea más económico. Por desgracia aquí no tenemos posibilidad de desarrollar este aspecto de la cuestión en forma más detallada.

§ 4. CRITERIOS GENERALES DE RESIDUOS EQUIVALENTES Y DE DIVISIBILIDAD

1. Todos los criterios de residuos equivalentes, así como los de divisibilidad construidos anteriormente, se ven un tanto artificiales y a primera vista parece que ellos, o al menos algunos de ellos, fueron hallados de casualidad, o bien son el resultado de pruebas y ensayos. En realidad esto no es así. Ocurre que existen procedimientos de construcción de criterios de divisibilidad y residuos equivalentes para cualquier número dado de antemano. Ellos se llaman, respectivamente, *criterios generales de divisibilidad* o *criterios generales de residuos equivalentes.*

Los criterios generales de divisibilidad son procedimientos de obtención de criterios concretos de divisibilidad. Por eso a estos últimos se les puede considerar como los resultados a los que llevan los criterios generales. Con tal punto de vista los criterios generales de divisibilidad son a los concretos absolutamente así, como el concreto es al resultado de su aplicación a cierto número, es decir, al residuo de la división del número dado a por el número dado m.

Los criterios generales de divisibilidad y residuos equivalentes semejan algoritmos, por lo demás, bastante originales: sus conclusiones y resultados tienen que volver a ser nuevamente algoritmos, precisamente, criterios concretos de divisibilidad o residuos equivalentes.

Pero, para tratar estos criterios generales como algoritmos, debemos estar seguros de que ellos poseen las condiciones necesarias de precisión, masividad y eficiencia.

Para hablar en detalle, señalando el criterio general de divisibilidad (lo mismo que el criterio general de residuos equivalentes) nosotros tenemos que verificar el cumplimiento de las siguientes condiciones. En primer lugar, para cualquier número m, él debe dar realmente un criterio de divisibilidad (de residuos equivalentes) por este número. Deberá, digamos así, «transformar» cada número natural m en criterio respectivo. Precisamente en esto reside su *eficiencia.* En segundo lugar, el criterio general tiene que ser *determinado*, es decir, aplicado al número dado m, él debe

llevar por un procedimiento bien definido a un criterio completamente concreto de divisibilidad (de residuos equivalentes) por este número. Por fin, en tercer lugar, el criterio debe ser *masivo* es decir, verdaderamente general, y dar criterios de divisibilidad o de residuos equivalentes para cualquier número natural concebido de antemano.

En este sentido, el procedimiento de construcción del criterio de residuos equivalentes, descripto en el p. 6 § 3, así como el procedimiento para hallar los criterios de divisibilidad descripto en el p. 9 § 3, no son criterios generales. En efecto, la indicación de las funciones que observan las condiciones necesarias es un proceso que no satisface, por ahora, ninguno de los requisitos de precisión, masividad y eficiencia.

En realidad, estos procedimientos no nos dan ninguna garantía de que la función necesaria será hallada; quiere decir que ellos carecen de eficiencia. Luego, si la función requerida precisamente existe, a ella se puede llegar por diferentes vías, sin hablar ya de que tales funciones pueden ser varias. O sea, estos procedimientos no tienen precisión. Finalmente, ellos tampoco son suficientes, y podría ser que para unos u otros valores concretos de m tampoco hallemos las funciones requeridas. En todo caso, por sí mismo el procedimiento no informa sobre esto. Así, para que el proceso descripto llegue a ser un algoritmo deberá ser completado aún con instrucciones precisas que garanticen la construcción de una función f_m, absolutamente determinada para cada número concreto m.

Este problema de «algoritmizar» la construcción de los criterios de divisibilidad puede ser resuelto incluso con bastante facilidad, pues los criterios generales de divisibilidad son conocidos desde hace mucho.

De hecho, uno de tales criterios generales de residuos equivalentes fue construido por nosotros en el p. 11 § 1 al tratar sobre la cuestión de la división residual. Se puede formular así: a cada número entero positivo m se le conforma un proceso de sustracción sucesiva de este número m hasta obtener uno menor que él (véase la última frase del p. 1 § 3). Tal conformación, está claro, posee todas las propiedades requeridas: de precisión (nosotros sabemos exactamente lo que conformamos al número m: el proceso de sustracciones sucesivas de m), de masividad (dicho proceso de sustraccio-

nes puede ser confrontado con cualquier m) y de eficiencia (tal intento siempre es exitoso). No obstante, el valor práctico del criterio general de residuos equivalentes descripto es muy pequeño.

Cierto perfeccionamiento del criterio general de residuos equivalentes, basado en la sustracción sucesiva, conduce al conocido proceso de división «sexagesimal» de números enteros. Este proceso también puede ser examinado como criterio general de residuos equivalentes. No está de más recordar que la aplastante mayoría de gente lo emplea, precisamente, para encontrar los residuos de la división. En este caso se razona siguiendo el esquema que transcribimos en dos variantes: en el lenguaje común de todos los días y en la lengua algorítmica.

En la lengua común	En la lengua algorítmica
1) Yo debo hallar el residuo de la división de a por el m dado;	El criterio general de residuos equivalentes comienza a transformar el número m;
2) para esto tengo que dividir por m;	el criterio general "nos da" el resultado de la transformación del número m; un criterio concreto de residuos equivalentes para la división por m, consistente en dividir por m directamente;
3) en este momento comienzo a efectuar la división de a por m...	el criterio concreto obtenido comienza a transformar el número a: la división con residuo por m;
4) ... divido y obtengo el residuo.	el criterio concreto nos lleva al objetivo: al residuo de la división de a por m.

En este razonamiento los tres primeros pasos son muy sencillos y por eso no puede asombrarnos que el cuarto paso, la ejecución de la división en sí, resulte tan voluminosa. La finalidad de los criterios generales de residuos equivalentes y divisibilidad, precisamente, es aligerar el cuarto paso a cuenta de que se perfeccione el segundo. Justamente esto es lo que se sobreentiende habitualmente al hablar de tales criterios.

2. El primer criterio general de divisibilidad (con más exactitud, incluso el de residuos equivalentes), histórica-

mento fue propuesto todavía a mediados del siglo XVII por el famoso matemático francés Pascal. Su esencia es la siguiente.

Sea m un número natural. Compongamos la sucesión de números

$$r_1, r_2, r_3, \ldots, \qquad (4.1)$$

suponiendo que

r_1 es igual a al residuo de la división de 10 por m,
r_2 » » » $10\, r_1$ por m,
r_3 » » » $10\, r_2$ por m,
etc.

Presentemos ahora el número natural arbitrario A en la forma

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10\, a_1 + a_0,$$

y determinemos la función

$$F_m(a) = \begin{cases} a_0 + r_1 a_1 + r_2 a_2 + \ldots + r_n a_n, & \text{si } 10^n \geqslant m, \\ \text{al residuo de la división de } A \text{ por } m & \text{si } 10^n < m \leqslant A, \\ \text{indeterminada,} & \text{si } A < m. \end{cases}$$

Problema 53. Verificar que la función F_m satisface las condiciones a)—d) del p. 10 § 3, para cualquier m.

Así, hemos construido un criterio de residuos equivalente, para la división por el número arbitrario m, o sea, un criterio general.

Problema 54. Formular los criterios de residuos equivalentes obtenidos del criterio general de Pascal en la división por:

a) 2, 5 y 10;
b) 4, 20 y 25;
c) 3 y 9;
d) 11;
e) 7.

Problema 55. Sean en la sucesión (4.1)

r_1, el residuo de dividir 100 por m,
r_2, » » » » $100\, r_1$ por m,
r_3, » » » » $100\, r_2$ por m,
etc.

Deducir de aquí un criterio general de residuos equivalentes, similar al de Pascal.

Problema 56. Deducir el criterio general de equirresidualidad en un sistema t^{nario} de numeración, análogo al criterio de Pascal.

3. En el p. 19 § 3 hemos hablado sobre las propiedades comparativas de los criterios de divisibilidad (o de residuos equivalentes) por un número determinado. Como el criterio general de divisibilidad tiene que proporcionarnos el criterio de divisibilidad por cualquier número natural, entonces, nada tiene de particular que para distintos números puede conducirnos a criterios de divisibilidad de la más diversa calidad.

Así, por ejemplo, el criterio general de Pascal junto con los criterios de residuos equivalentes, completamente admisibles para la división por 3 y 11, nos da un criterio de residuos equivalentes para la división por 7, muy voluminoso y de difícil aplicación (véase el problema 54, e)).

Con relación a esto, a propósito de los criterios generales de divisibilidad y residuos equivalentes, se pueden enunciar consideraciones semejantes a las que se expusieron en el p. 19 § 3 durante el examen de la calidad de los criterios concretos de divisibilidad. En este sentido se considerará óptimo el criterio general de divisibilidad (de residuos equivalentes) que, aplicado a cualquier entero positivo dado de antemano m, nos dé el mejor criterio de divisibilidad (de residuos equivalentes) por este m. El lector comprenderá que hallar el criterio general de divisibilidad más acertado es una cuestión que está lejos no sólo de ser resuelta, sino incluso de un planteo riguroso.

§ 5. DIVISIBILIDAD DE POTENCIAS

1. Comencemos por la descripción de un proceso al que se podría llamar «criterio muy general de residuos equivalentes».

Sea k cierto número natural y r el residuo de la división de t^k por m:

$$t^k = mq + r \quad (0 \leqslant r < m).$$

Por el corolario del teorema 20 (véase el p. 3 § 2), para cualquier n, los números r^n y t^{kn}, al ser divididos por m también deberán ser equirresiduales.

Fraccionemos ahora el número arbitrario A de derecha a izquierda, en «grupos» k^{narios}, o sea, presentémoslo en la forma

$$A = a_n t^{kn} + a_{n-1} t^{k(n-1)} + \ldots + a_1 t^k + a_0,$$

donde

$$0 \leqslant a_i < t^k \text{ para } i = 0, 1, \ldots, n,$$

y pongamos que

$$f(A) = \begin{cases} a_n r^n + a_{n-1} r^{n-1} + \ldots + a_1 r + a_0, & \text{si } A \geqslant t^k, \\ \text{al residuo de dividir } A \text{ por } m, & \text{si } m \leqslant A < t^k, \\ \text{indeterminada}, & \text{si } A < m. \end{cases}$$

Es evidente que en casos similares, como antes, el proceso de construcción de los números

$$A_0 = A,\ A_1 = f(A_0),\ A_2 = f(A_1),\ \ldots$$

es un criterio de residuos equivalentes.

Problema 57. Cerciorarse, no obstante, que esto realmente es así.

Problema 58. Suponiendo que $t = 10$ y $k = 2$, hallar el residuo de la división del número 1 048 576 por 7.

Problema 59. Cerciorarse de que el criterio de residuos equivalentes que acabamos de escribir sólo es una forma más clara de aquella generalización del criterio de Pascal mencionado en el problema 56.

2. Hablando formalmente, al componer en el p.1 el criterio general de equirresidualidad, aplicamos las propiedades de las potencias atinentes a su divisibilidad. Sin embargo, la cuestión relativa a dicha divisibilidad es, en esencia, algo que trata sobre la división de ciertos productos. Por eso, en principio, también se logró resolver esto tomando como base los resultados de § 2. Simultáneamente, la realización práctica del criterio de equirresidualidad obtenido para unas u otras combinaciones de los valores de los números t y m puede conducir a grandes valores de k y r, tales, que el cálculo de los valores de la función f requiera llevar a cabo una considerable cantidad de cómputos, que incluso podría superar, en volumen, las operaciones de la división directa por m.

Está claro que el cálculo de los valores de la función f resultará tanto más sencillo, cuanto menores sean los valores de los números k y r. Se sobreentiende que los más convenientes, en este sentido, son cuando $r = 1$. Entonces, el valor de f se obtiene como resultado de la ejecución de una operación más fácil: la adición.

Según el teorema 22, este caso ($r = 1$) tiene lugar, única y exclusivamente cuando $(t^k - 1) : m$ o, con otras palabras, cuando t^k, dividido por m, deja como residuo 1. Surge el interrogante: ¿hallaremos para los datos t y m tal k que $(t^k - 1) : m$?

Todo lo dicho induce a estudiar la división de las potencias con más detalle.

3. Ampliemos un tanto nuestros conocimientos en el campo de la teoría de los números.

TEOREMA 24 (de Fermat). *Si el número p es primo, la diferencia $a^p - a$ es divisible por él.*

No se debe confundir el denominado «pequeño teorema» de Fermat con su «gran teorema». Este último afirma que para un entero $n > 2$ no existen enteros a, b y c tales que $a^n + b^n = c^n$. A despecho de numerosas tentativas, hasta ahora el gran teorema no fue ni demostrado ni refutado.

Corolario. Si p es primo y a indivisible por él, entonces $a^{p-1} - 1$ es divisible por p.

Problema 60. Presentar un ejemplo donde se manifieste que tanto el teorema 24 como su corolario para un p compuesto, hablando en general, no son correctos.

Problema 61. Demostrar el teorema de Fermat basándose en el resultado del problema 26.

Supongamos que el número natural m tiene la descomposición canónica:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_h^{\alpha_h}; \qquad (5.1)$$

pongamos que

$$\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_h^{\alpha_h - 1}(p_h - 1). \qquad (5.2)$$

Las fórmulas (5.1) y (5.2) conforman para cada m natural un número completamente determinado $\varphi(m)$. Esto quiere decir que podemos hablar de función φ del argumento natural.

DEFINICION La función φ determinada antes se llama *función de Euler.*

La función de Euler juega un papel extraordinariamente importante en muchas cuestiones de la teoría de los números. Incluso en este libro indicaremos varias aplicaciones de ella.

TEOREMA 25 *Para m_1 y m_2, primos entre sí, tiene lugar la siguiente igualdad:*

$$\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2).$$

Problema 62. Calcular $\varphi(12)$, $\varphi(120)$ y $\varphi(1000)$.

Problema 63. Determinar todos los números m para los cuales:

a) $\varphi(m) = 10$,

b) $\varphi(m) = 8$.

Problema 64. Demostrar que no existe tal m, para el que $\varphi(m) = 14$.

Problema 65. Demostrar que $\varphi(m)$ es igual a la cantidad de números naturales primos entre sí con m y menores que m. Esta propiedad de la función de Euler tiene extraordinaria importancia. Frecuentemente ella es confundida con la definición de la función.

TEOREMA 26 (teorema de Euler). *Si los números a y m son primos entre sí, $a^{\varphi(m)} - 1$ es divisible por m.*

Los residuos de la división de un mismo dividendo por diferentes divisores, se hallan ligados entre sí de un modo bastante complejo. Del teorema de Euler se puede obtener la dependencia, de principal importancia para nosotros, que tienen los residuos de la división por factores primos entre sí, con la división por el producto de ellos.

Problema 66. Sean $(m_1, m_2) = 1$, a_1 y a_2 números equirresiduales con A para las divisiones por m_1 y m_2, respectivamente. Entonces, en la división por m_1m_2, el número

$$(a_1m_2 + a_2m_1)(m_1 + m_2)^{\varphi(m_1m_2)-1}$$

será equirresidual con A.

4. A base de los hechos establecidos podemos formular el criterio general de los residuos equivalentes para un divisor arbitrario m, en un sistema también arbitrario de numera-

ción t, en aquella forma clara y suficientemente manejable, de la que se habló en el p. 1.

Les recordamos nuevamente que cualquier criterio de equirresidualidad es un algoritmo, o sea, un determinado proceso y, por eso, el carácter de cualquier descripción de él deberá ser una narración en desarrollo.

Así, tenemos los números m y t. Presentemos m en la forma de un producto $m = m_1 m_2$ tal que $(m_1 t) = 1$ y para cierta potencia k tenga lugar la divisibilidad $t^k : m_2$. Según el teorema 18, tal presentación es posible. En vigor del problema 66, el asunto que trata sobre la equirresidualidad para la división por $m_1 m_2$ puede ser reducida a una cuestión análoga en la división por m_1 y m_2. Pero el criterio de equirresidualidad para m_2 lo contiene el teorema 21, y el de equirresidualidad para m_1, el teorema 22. Después de aplicar estos criterios de residuos equivalentes debemos utilizar el resultado del problema 66.

Por ejemplo, en el caso de hallar el criterio de equirresidualidad para la división por 12 en un sistema de numeración decimal, evidentemente, $m_1 = 3$, $m_2 = 4$, y $k = 2$.

El proceso descripto es criterio general de residuos equivalentes, en el sentido de que él, para cualquier m, brinda cierto criterio concreto de equirresidualidad. Esto se desprende de la algoritmizabilidad de la construcción de la descomposición canónica del número (véase el p. 9 § 3).

Nos queda formular con claridad el criterio de equirresidualidad señalado para la división por m_1, valiéndonos de la posibilidad de determinar el índice k, basándonos en el teorema de Euler.

5. Aplicando los teoremas demostrados construyamos varios criterios generales de divisibilidad y residuos equivalentes.

Fijemos el número natural m y presentemos el número A en la forma

$$A = a_0 + a_1 10^{\varphi(m)} + a_2 10^{2\varphi(m)} + \ldots + a_h 10^{h\varphi(m)},$$

donde

$$0 \leqslant a_0, a_1, a_2, \ldots, a_k \leqslant 10^{\varphi(m)},$$

o sea, los números a_i $(i = 0, 1, \ldots, k)$ son $\varphi(m)$-narios.

La función

$F(A) =$

$$= \begin{cases} a_0 + a_1 + \ldots + a_n, & \text{si } A \geqslant 10^{\varphi(m)}, \\ \text{al residuo de la división de } A \text{ por } m, & \text{si } m \leqslant A < 10^{\varphi(m)}, \\ \text{indeterminada}, & \text{si } A < m, \end{cases}$$

establece, como es fácil de comprobar, cierto criterio general de residuos equivalentes.

Problema 67. Verificar esta circunstancia.

TEOREMA 27. *Si los números a y m son primos entre sí y los k_1 y k_2, equirresiduales, en la división por $\varphi(m)$, los números a^{k_1} y a^{k_2} son equirresiduales en la división por m.*

Problema 68. Formular los criterios concretos de equirresidualidad para la división por 7, 11 y 13, obtenidos a base de este criterio general de residuos equivalentes.

Problema 69. Formular el criterio análogo general de equirresidualidad para un sistema t^{nario} arbitrario de numeración. Cerciorarse de que el criterio general de residuos equivalentes, así obtenido, por su formulación no depende de la base t del sistema numérico.

Problema 70. Demostrar que $(n^{13} - n) \vdots 2730$.

6. En muchos casos el criterio general de residuos equivalentes no es, por decirlo así, «suficientemente económico», ya que, hablando en general, el número $\varphi(m)$ puede resultar demasiado grande. De ahí que, al emplear este criterio nos vemos obligados, por un lado, a sumar enormes guarismos y, por el otro, en este caso, a dividir los números $\varphi(m)$-narios directamente por m (o emplear algún criterio distinto de divisibilidad y residuos equivalentes). Por eso, en lugar de $\varphi(m)$ es deseable probar otro exponente menor. En una serie de casos esto se consigue hacer. Por ejemplo, para $m = 37$, se puede tomar 3 en lugar de $\varphi(m) = 36$, ya que 1000, en la división por 37 deja un uno como residuo; para $m = 11$ se puede tomar 2 en lugar de $\varphi(m) = 10$; etc.

DEFINICIÓN. El número δ mínimo, para el cual al dividir a^δ por m queda como residuo 1, se llama *exponente, al que le pertenece el número a para la división residual por m.*

Con mayor frecuencia este número es llamado *exponente, al que pertenece a con el módulo m.*

Evidentemente, cualesquiera que sean los números primos entre sí a y m, el exponente δ, al que pertenece a en

la división por m, no supera $\varphi(m)$. Este exponente se puede tomar, precisamente, en lugar de $\varphi(m)$, al formular el criterio general de divisibilidad del p. 5.

Problema 71. Modificar el criterio general de divisibilidad construido, empleando en lugar de $\varphi(m)$ el exponente al que le pertenece 10 en la división residual por m.

Problema 72. Lo mismo para un sistema t^{nario} de numeración.

7. El exponente, al que le pertenece el número a en la división por m, hablando en general, también puede ser igual a $\varphi(m)$. Por ejemplo, la sucesión de los residuos de dividir las potencias del número dos por 11, será

$$2,\ 4,\ 8,\ 5,\ 10,\ 9,\ 7,\ 3,\ 6,\ 1,$$

tal, que al dividir por 11, el número 2 pertenezca al exponente 10. Esto significa que para emplear el criterio de equirresiduatidad del p. 5, en este caso, nos vemos obligados a tomar $k = 10 = \varphi(11)$.

No obstante, en muchos casos basta el exponente ${}^1/_2\varphi(m)$. Sea m, por ejemplo, exponente de un número primo: $m = p^\alpha$ y $p \neq 2$. Entonces $\varphi(m) = p^{\alpha-1}(p-1)$, y el teorema de Euler adquiere la forma: $(a^{p^{\alpha-1}(p-1)} - 1) \vdots p^\alpha$ para $(a, p) = 1$. Dado que el número $p^{\alpha-1}(p-1)$ es par, el último dividendo resulta una diferencia de cuadrados, y nosotros tenemos que

$$(a^{1/2p^{\alpha-1}(p-1)} + 1)(a^{1/2p^{\alpha-1}(p-1)} - 1) \vdots p^\alpha.$$

Como $p \neq 2$, ambos factores no pueden simultáneamente ser divisibles por p. Esto significa que lo es, o bien $a^{1/2\varphi(m)} + 1$, o bien $a^{1/2\varphi(m)} - 1$. En el primer caso nos vemos en las condiciones del teorema 23, donde $k = {}^1/_2\varphi(m)$, y en el segundo, en las del teorema 22, con el mismo $k = {}^1/_2\varphi(m)$.

8. El empleo de la función y el teorema de Euler no queda limitado a los criterios de divisibilidad. Por su intermedio se pueden resolver, por ejemplo, ecuaciones con números enteros.

TEOREMA 28. *Si los números a y b son primos entre sí, la ecuación*

$$ax + by = c \qquad (5.3)$$

siempre puede ser resuelta en números enteros y todas las parejas de números (x_t, y_t) donde

$$x_t = c\,a^{\varphi(b)-1} + bt,$$

$$y_t = c\,\frac{1 - a^{\varphi(b)}}{b} - at$$

(t es cualquier número entero) serán sus soluciones completas.

Problema 73. Demostrar un teorema análogo al 28 sin suponer que los números a y b son primos entre sí.

Problema 74. Hallar el procedimiento de resolución, en números enteros, de las ecuaciones del tipo (5.3), basándose en el resultado del problema 29, b).

Problema 75. Resolver en números enteros las ecuaciones

a) $5x + 7y = 9$,

b) $25x + 13y = 8$.

9. TEOREMA 29. *Sean m y 10 primos entre sí y k equirresidual con $10^{\varphi(m)-1}$ en la división por m. Entonces los números $10a + b$ y $a + kb$ serán equidivisibles por m.*

Basándose en este teorema, se puede construir el siguiente criterio general de divisibilidad. Designemos con k al residuo de la división residual de $10^{\varphi(m)-1}$ por m, presentemos el número arbitrario A en la forma $10a + b$ $(0 \leqslant b < < 10)$ y pongamos que:

$$F(A) = \begin{cases} a + kb & \text{para } A > a + kb, \\ \text{al residuo de la división de } A \text{ por } m & \text{para } m \leqslant A < a + kb, \\ \text{indeterminada,} & \text{para } A < m. \end{cases}$$

Si k resulta demasiado grande (próximo a m), en su lugar es conveniente colocar, en la formulación del respectivo criterio, $k - m$.

Problema 76. Verificar, para la función F, el cumplimiento de las condiciones a)—c) del p. 10 § 3 y d*) del p. 15 § 3.

Problema 77. A base del criterio general de divisibilidad que acabamos de construir, deducir el criterio de divisibilidad por los números 17, 19, 27, 31, y 49.

Problema 78. Construir un criterio general de divisibilidad análogo, representando al número natural arbitrario en la forma $100a + b$ $(0 \leqslant b < 100)$, y deducir de él los criterios de divisibilidad por 17, 43, 49, 67, 101 y 199.

Problema 79. Construir un criterio análogo de divisibilidad en un sistema t^{nario} de numeración.

Problema 80. A base del criterio general de divisibilidad construido, deducir criterios concretos de divisibilidad para la división por:

a) 21, en el sistema octóneo u octonario de numeración;

b) 31, en el sistema duodecimal de numeración.

1. Es suficiente señalar que $a = a \cdot 1$.

2. Por condición, se hallarán d_1 y d_2 tales, que $a = bd_1$ y $b = cd_2$. Pero entonces, $a = cd_1d_2$, es decir, $a \vdots c$.

3. Nosotros tenemos que $a = bc_1$ y $b = ac_2$, de donde resulta que $a = ac_1c_2$, es decir, $c_1c_2 = 1$. Como los números c_1 y c_2 son enteros por condición, en'onces o bien $c_1 = c_2 = 1$, o bien $c_1 = c_2 = -1$. En el imer caso $a = b$ y en el segundo $a = -b$.

4. Sea $a = bc$. Si $|c| \geqslant 1$, entonces, por cuanto $|b| > |a|$, también $|bc| > |a|$, lo que contradice la hipótesis. Quiere decir que $|c| < 1$, y como el número c es entero por condición, $c = 0$, por lo que también $a = 0$.

5. Evidentemente, de $a = bc$ se deduce que $|a| = |b|\,|c|$ y de $|a| = |b|\,|c|$, que $a = bc$ o $a = b(-c)$, además, los números c, $-c$ y $|c|$ son enteros o no, simultáneamente.

6. En efecto, sean

$$a_1 = bc_1,$$
$$a_2 = bc_2,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot$$
$$a_n = bc_n,$$

donde todos los números $c_1, c_2, \ldots, c_n$ son enteros. Sumando por miembros estas igualdades obtenemos

$$a_1 + a_2 + \ldots + a_n = b\,(c_1 + c_2 + \ldots + c_n).$$

Lo que se halla entre paréntesis es un número entero, quedando demostrado con ello justamente lo que se pedía.

8. La demostración se efectúa por el absurdo. Supongamos que la cantidad de números primos es finita, de modo que todos ellos puedan ser escritos:

$$p_1, p_2, \ldots, p_n. \qquad \text{(Demost. 1)}$$

Designamos por P al producto de todos estos números y examinamos la diferencia $P - 1$. Esta supera a cada uno de los números primos enumerados en la notación (Demost. 1) por lo que no puede ser número primo. De tal modo, ella es divisible como mínimo por un número primo p_k. Pero incluso P lo es por p_k. Por consiguiente, a base del corolario

del teorema 6, también $1 : p_k$, de donde $p_k = 1$, lo cual contradice el hecho de que el número p_k sea primo (véase la pág. 24).

La demostración expuesta de la infinidad del conjunto de números primos fue hallada por Euclides (en el siglo IV a.n.e.).

9. Si los números a y p son primos entre sí, entonces el teorema queda demostrado. En caso contrario ambos serán divisibles por un mismo número, distinto de la unidad. Como p es primo, tal número puede ser solamente p. Quiere decir que en este caso $a : p$ y esto es precisamente lo que se pedía.

10. Dividiendo con residuo M por m obtenemos

$$M = mq + r,$$

donde $0 \leqslant r < m$. Como M y m son divisibles por a y b, entonces, según el corolario del teorema 6, también el número r lo deberá ser, con lo cual resulta múltiplo común de estos números. Pero $r < m$ y m es el mínimo común múltiplo positivo de a y b. Quiere decir que r no puede ser positivo, de tal modo, $r = 0$. Por eso $M : m$.

11. Aceptemos que los números a y b son primos entre sí y m es su mínimo común múltiplo. Como $ab : a$ y $ab : b$, entonces, por el teorema anterior, $ab : m$. Sea $ab = mk$. Pongamos que $m = ac$. Entonces $ab = ack$, es decir, $b = ck$, así que $b : k$. Exactamente de igual manera podemos persuadirnos de que también $a : k$. Dado que a y b son primos entre sí por condición, $k = 1$, y esto quiere decir, precisamente, que $m = ab$.

12. Llamemos m al mínimo común míltiplo de los números b y c. Por el teorema precedente $m = bc$. Prosiguiendo, por condición $ab : c$, además, evidentemente, $ab : b$. Quiere decir, según el teorema 10, que $ab : bc$, es decir, que $ab = bck$ o, después de simplificar por b, que $a = ck$, y esto es justamente lo que se pedía.

13. La demostración se efectúa por inducción según el número de factores. Habiendo uno solo, entonces el teorema es trivial. Supongamos que el teorema fue demostrado para cualquier producto de n factores. Sea $a_1a_2 \ldots a_na_{n+1} : p$. Designemos $a_1a_2 \ldots a_n$ por A. En este caso $Aa_{n+1} : p$. Si $a_{n+1} : p$, el teorema queda demostrado, en caso contrario, a_{n+1} y p, según el teorema 9, son primos entre sí. Pero entonces, por lo anterior, $A : p$. Dado que A es un producto

de n factores, uno de ellos, por consideraciones de inducción, tiene que ser divisible por p. El teorema queda demostrado.

Corolario. Todo el quebrado representa un número entero, es decir, su numerador es divisible por el denominador. Consideremos al numerador producto de dos factores: p y $1 \cdot 2 \ldots (p-1) = (p-1)!$

Ninguno de los factores del denominador del quebrado es divisible por p. De ahí que, según el teorema anterior, tampoco lo sea todo el denominador. Pero entonces, de acuerdo al teorema 9, él y p son primos entre sí. Por eso, deberá ser divisible por el denominador el segundo factor del numerador. Llamando q al cociente de esta división, $C_p^h = pq$ y lo exigido queda demostrado.

14. Probemos al principio que cualquier número diferente de la unidad *puede* ser descopuesto en factores simples. Supongamos que todos los números menores de N pueden ser descompuestos así. Si N es primo, entonces, él se descompone automáticamente en producto de primos (compuesto precisamente, de un solo factor, del propio número N) y el teorema queda demostrado. Sean ahora N compuesto, N_1 un divisor suyo, diferente tanto de él como de la unidad, y N_2 el cociente de dividir N por N_1. Entonces, $N = N_1N_2$ y además, como es fácil comprobar, $1 < N_2 < N$. Dado que N_1 y N_2 son menores de N, entonces, por hipótesis, ellos pueden ser descompuestos en productos de factores primos. Sean estas descomposiciones $N_1 = p_1p_2 \ldots p_k$ y $N_2 = q_1q_2 \ldots q_l$. Entonces, $p_1p_2 \ldots p_kq_1q_2 \ldots q_l$ es la doscomposición buscada del número N. De tal modo, la posibilidad de descomponer queda demostrada.

Pasamos a demostrar *la unicidad* de la descomposición. Aceptemos que se nos hayan dado dos descomposiciones del número N en factores primos: $p_1p_2 \ldots p_k$ y $q_1q_2 \ldots q_l$. Evidentemente,

$$p_1p_2 \ldots p_k = q_1q_2 \ldots q_l. \qquad \text{(Demost. 2)}$$

Como $q_1q_2 \ldots q_l$ es divisible por p_1, entonces, de acuerdo al teorema anterior, al menos uno de los números de q_1, $q_2, \ldots, q_l$ será divisible por p_1. Aceptemos que $q_1 : p_1$ (el hecho de que consideremos divisible por p_1 precisamente al primer factor del segundo miembro de (Demost. 2) no es ninguna hipótesis complementaria, ya que tenemos derecho a cambiar de lugar los factores y designar por q_1 precisa-

mente a aquel que es divisible por p_1). Dado que el número q_1 es primo, entonces, esto es factible solamente para $p_1 = q_1$. Simplificando por p_1 la igualdad (Demost. 2), obtenemos

$$p_2 p_3 \ldots p_k = q_2 q_3 \ldots q_l. \qquad \text{(Demost. 3)}$$

En forma análoga a la anterior nos convencemos de que uno de los números de $q_2, q_3, \ldots, q_l$ (por ejemplo, q_2) es divisible por p_2 y, por eso, $p_2 = q_2$. Simplificando la igualdad (Demost. 3) por p_2 disminuimos la cantidad de factores de sus miembros aún en una unidad. Tal proceso de simplificación, evidentemente, se puede prolongar hasta que uno de los productos quede completamente simplificado. Sea el primero en simplificarse el producto ubicado en el primer miembro de (Demost. 2). El producto ubicado en el segundo miembro de (Demost. 2) también quedará íntegramente simplificado, de lo contrario obtendríamos una igualdad del tipo

$$1 = q_{k+1} \ldots q_l,$$

cosa imposible, ya que la unidad no es divisible por ningún número primo. Con lo cual nosotros obtenemos también que

$$p_1 = q_1,\ p_2 = q_2,\ \ldots,\ p_k = q_k.$$

El teorema queda enteramente demostrado.

15. Sean $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ y $q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$, respectivamente, descomposiciones canónicas de los números a y b; y d, un divisor común de ellos. Si $d \neq 1$, será divisible por un número primo p. Entonces, de acuerdo al teorema 3, $a \vdots p$ y $b \vdots p$, de manera que p se halla tanto entre los números $p_1, p_2, \ldots, p_k$, como entre los $q_1, q_2, \ldots, q_l$. Por eso, entre los números primos que integran la descomposición canónica a habrá uno que integre la canónica b.

A la inversa, si a y b son primos entre sí y p integra la descomposición canónica a, entonces, b no será divisible por p y p no integrará la descomposición canónica b.

16. Necesidad. Como $a \vdots p_i^{\alpha_i}$ $(i = 1, 2, \ldots, k)$, de $b \vdots a$ obtenemos lo requerido mediante la simple referencia al teorema 2.

La suficiencia se demuestra por inducción. La divisibilidad $b \vdots p_1^{\alpha_1}$ es una de las condiciones. Supongamos estable-

cido ya por nosotros que

$$b \vdots p_1^{\alpha_1} \dots p_l^{\alpha_l} \quad (1 \leqslant l < k).$$

Además, disponemos de la divisibilidad $b \vdots p_{l+1}^{\alpha_{l+1}}$. Como los números $p_l^{\alpha_1} \dots p_l^{\alpha_l}$ y $p_{l+1}^{\alpha_{l+1}}$, según el teorema anterior, son primos entre sí, nosotros podemos emplear el corolario del teorema 11, por el que

$$b \vdots p_1^{\alpha_1} \dots p_l^{\alpha_l} p_{l+1}^{\alpha_{l+1}}.$$

Así, el paso inductivo queda fundamentado.

17. Necesidad. Pongamos que $a \vdots b$. Del teorema 13 se deduce que cada divisor primo b es un divisor primo de a. De tal modo, b posee la forma

$$p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

donde $0 \leqslant \beta_1$, $0 \leqslant \beta_2$, ..., $0 \leqslant \beta_k$. Supongamos que $\beta_1 > > \alpha_1$. Como

$$\frac{a}{b} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}{p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}} = \frac{p_2^{\alpha_2} \dots p_k^{\alpha_k}}{p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \dots p_k^{\beta_k}}$$

es un número entero, el número del último quebrado deberá ser divisible por el denominador y con más razón por $p_1^{\beta_1 - \alpha_1}$. Pero entonces, según el teorema 13, al menos uno de los números p_2, ..., p_k, deberá ser divisible por p_1, lo que no puede ser. Quiere decir que $\beta_1 \leqslant \alpha_1$. Como para nosotros es] indiferente la numeración de los divisores primos de a, hemos probado con ello que también $\beta_2 \leqslant \alpha_2$, ..., $\beta_k \leqslant \alpha_k$ La necesidad quedó establecida.

Para demostrar *la suficiencia* señalamos que si b tiene la forma indicada, entonces

$$a = b p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_k^{\alpha_k - \beta_k}.$$

18. Escribamos la descomposición canónica de los números m y t:

$$m = p_1^{\alpha_1} \dots p_n^{\alpha_n}, \; t = q_1^{\beta_1} \dots q_l^{\beta_l}.$$

Escojamos entre los primos p_1, ..., p_n aquellos que dividan t, o sea, que se hallen entre q_1, ..., q_l. Para ser precisos, aceptemos que p_1, ..., p_r sean respectivamente

iguales a $q_1, \ldots, q_r$. Pongamos entonces que

$$m_2 = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \text{ y } m_1 = p_{r+1}^{\alpha_{r+1}} \ldots p_n^{\alpha_n}.$$

Según el teorema 15, $(m_1, t) = 1$. Además, tomemos el número natural k que no sería inferior a ninguna de las relaciones

$$\frac{\alpha_1}{\beta_1}, \ldots, \frac{\alpha_r}{\beta_r}.$$

Esto significa que para $i = 1, \ldots, r$, $k\beta_i \geqslant \alpha_i$, por lo que, de acuerdo con el teorema 17, $t^k \vdots m_2$.

19. Necesidad. Sean

$$a = mq_1 + r_1 \quad (0 \leqslant r_1 < m), \qquad \text{(Demost. 4)}$$
$$b = mq_2 + r_2 \quad (0 \leqslant r_2 < m). \qquad \text{(Demost. 5)}$$

Como a y b son equirresiduales, $r_1 = r_2$. Esto significa que

$$a - b = m(q_1 - q_2),$$

es decir, $(a - b) \vdots m$.

Suficiencia. Sea $(a - b) \vdots m$. Dividiendo a y b por m obtenemos (Demost. 4) y (Demost. 5). Además,

$$a - b = m(q_1 - q_2) + r_1 - r_2,$$

es decir,

$$(a - b) - m(q_1 - q_2) = r_1 - r_2.$$

Según el teorema 6, $(r_1 - r_2) \vdots m$. Pero $|r_1 - r_2| < m$. O sea, que por el teorema 4, $r_1 - r_2 = 0$ ó $r_1 = r_2$, y esto es precisamente lo que se pedía.

20. De la condición a base del teorema 16 tenemos

$$\left.\begin{array}{l} a_1 = b_1 + mq_1 \\ a_2 = b_2 + mq_2, \\ \cdots\cdots\cdots \\ a_n = b_n + mq_n. \end{array}\right\} \qquad \text{(Demost. 6)}$$

Sumando miembro a miembro estas igualdades, después de simples transformaciones, obtenemos

$$(a_1 + a_2 + \ldots + a_n) - (b_1 + b_2 + \ldots + b_n) = \\ = m(q_1 + q_2 + \ldots + q_n),$$

que por el teorema 19 significa que precisamente las sumas son equirresiduales.

Para demostrar que los productos son equirresiduales señalamos la siguiente identidad:

$$(k + bm)(p + qm) = kp + (pq + lp + lqm)m.$$

De ella se deduce que el producto de dos números del género $a + bm$ resulta nuevamente un número del mismo género. Por eso, razonando inductivamente, nos convencemos de que el producto de cualquier cantidad de números tipo $a + bm$ es un número de igual tipo.

Multiplicando término por término todas las igualdades (Demost. 6) y aplicando al segundo miembro los razonamientos efectuados obtenemos

$$a_1a_2 \ldots a_n = b_1b_2 \ldots b_n + mt,$$

donde t es un número entero. De tal modo, el hecho de que los productos son equirresiduales queda probado.

21. Necesidad. Si el algoritmo descripto es un criterio de residuos equivalentes para la división por m, entonces, para ella, también los números A y b deberán ser equirresiduales. En particular, esto será así si $A = t^k + b$. Pero esto significa que $A - b = t^k \vdots m$.

Suficiencia. En nuestras designaciones $A - b = at^k$, es decir, los números A y b son equirresiduales en la división por m. Si $t^k \vdots m$, entonces para ésta, por el corolario del teorema 17, ellos también son equirresiduales. Por eso, en este caso, la sucesión $A_0, A_1, \ldots$, construida con el algoritmo, está compuesta por números que son equirresiduales en la división por m. Así pues, el proceso de construcción de dicha sucesión es criterio de equirresidualidad para la división por m.

22. Necesidad. Si el algoritmo descripto es realmente un criterio de equirresidualidad para la división por m, el mismo, en particular, también deberá ser aplicable al número $A = t^k + a_0$. Aquí, $f(A) = a_0 + 1$ y la equirresidualidad de los números A y $f(A)$, en la división por m, significa que $(t^k - 1) \vdots m$.

Suficiencia. Sea $A \geqslant t^k$. Entonces, de la definición de la función f se desprende que

$$A - f(A) = a_n(t^{kn} - 1) + a_{n-1}(t^{k(n-1)} - 1) + \ldots$$
$$\ldots + a_1(t^k - 1).$$

Aquí, cada sumando (véase, por ejemplo, el problema 22, p. e)) es divisible por $t^k - 1$. Esto significa que si $(t^k - 1) \vdots m$, también $A - f(A) \vdots m$. La equirresidualidad de los restantes términos de la sucesión (3.4) y también de sus términos, si ella comienza por el número $A < t^k$, se desprende de su construcción.

23. Necesidad. En el caso de $A = t^k + a_0$, la equirresidualidad de los números A y $f(A) = a_0 - 1$ en la división por m, nos da $(t^k + 1) \vdots m$.

Suficiencia. En nuestro caso tenemos que para $A \geqslant t^k$

$$A - f(A) = a_n (t^{kn} \pm 1) + a_{n-1} (t^{k(n-1)} \mp 1) + \ldots$$
$$\ldots + a_1 (t^k + 1) \qquad \text{(Demost. 7)}$$

(aquí, el signo «más» se halla en el término que corresponde al coeficiente impar con k como exponente, y el «menos», al coeficiente par). Según los p. e) y f) del problema 22, la expresión $t^{kr} + 1$ para un r impar es divisible por $t^k + 1$, y la $t^{kr} - 1$, para un r par, también es divisible por $t^k + 1$. Eso significa que si $(t_k + 1) \vdots m$, en (Demost. 7) cada término es divisible por m, contando desde la derecha, y, por lo tanto, también lo es toda la diferencia $A - f(A)$. Así pues, los números A y $f(A)$, en la división por m, resultan equirresiduales. La equirresidualidad de los términos restantes de la sucesión (3.4), así como de los propios términos de esta última, si ella comienza por el número $A < t^k$, se desprende directamente de su construcción.

24. La demostración se efectúa en forma inductiva por a. Para $a = 1$

$$a^p - a = 1 - 1 = 0,$$

y $0 \vdots p$.

Supongamos que $a^p - a$ es divisible por p y demostremos que $(a + 1)^p - (a + 1)$ también es divisible por p. En efecto, descomponiendo $(a + 1)^p$ por la fórmula del binomio de Newton tenemos

$$(a+1)^p - (a+1) = a^p + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \ldots$$
$$\ldots + C_p^{p-1} a + 1 - a - 1 = a^p - a + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \ldots$$
$$\ldots + C_p^{p-1} a. \qquad \text{(Demost. 8)}.$$

$a^p - a$ es divisible entre p por hipótesis. De acuerdo con el

corolario del teorema 13, C_p^k $(1 \leqslant k \leqslant p-1)$ igualmente es divisible por p. Por consiguiente, entre p es divisible cada sumando del segundo miembro de la relación (Demost. 8), de ahí que (teorema 6) también lo sea toda la suma.

Hemos fundamentado el paso inductivo y demostrado todo el teorema.

Corolario. Por el teorema de Fermat

$$a^p - a = a\,(p^{p-2} - 1) \vdots p.$$

Si a, en este caso, no es divisible por p, según el teorema 13, por p deberá dividirse $a^{p-1} - 1$.

25. Sean $m_1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ y $m_2 = q_1^{\beta_1} \ldots q_l^{\beta_l}$. Por el teorema 15 cada uno de los números $p_1, \ldots, p_k$ es diferente de cada uno de los números $q_1, \ldots, q_l$. Quiere decir que la descomposición canónica $m_1 m_2$ será $p_1^{\alpha_1} \ldots p_k^{\alpha_k} q_1^{\beta_1} \ldots q_l^{\beta_l}$. Por eso

$$\varphi(m_1 m_2) = p_1^{\alpha_1 - 1}(p_1 - 1) \ldots p_k^{\alpha_k - 1} \times$$
$$\times (p_k - 1) \cdot q_1^{\beta_1 - 1}(q_1 - 1) \ldots q_l^{\beta_l - 1}(q_l - 1),$$

es decir,

$$\varphi(m_1 m_2) = \varphi(m_1)\,\varphi(m_2).$$

26. Demostremos al principio en forma deductiva según α, que $a^{p^{\alpha-1}(p-1)} - 1$ es divisible por p^α. Para $\alpha = 1$ la afirmación demostrada, evidentemente, es corolario del teorema de Fermat, cuya certeza ya fue establecida. De tal modo, la base de la inducción queda demostrada.

Supongamos ahora que $(a^{p^{\alpha-1}(p-1)} - 1) \vdots p^\alpha$ y examinemos la expresión $a^{p^\alpha(p-1)} - 1$. Nosotros deberemos demostrar que ella es divisible por $p^{\alpha+1}$. Pero

$$a^{p^\alpha(p-1)} - 1 = (a^{p^{\alpha-1}(p-1)})^p - 1.$$

Dado que $a^{p^{\alpha-1}(p-1)} - 1$, según hipótesis, es divisible por p^α, el número $a^{p^{\alpha-1}(p-1)}$ tiene la forma $Np^\alpha + 1$. Esto significa que

$$a^{p^\alpha(p-1)} - 1 = (Np^\alpha + 1)^p - 1,$$

es decir, por la fórmula del binomio,

$$a^{p^\alpha(p-1)} - 1 = N^p p^{\alpha p} + C_p^1 N^{p-1} p^{\alpha(p-1)} + \ldots$$
$$\ldots + C_p^{p-1} N p^\alpha + 1 - 1.$$

El primer sumando de la última suma es divisible por $p^{\alpha+1}$, ya que lo es por $p^{\alpha p}$ y $\alpha p \geqslant \alpha + 1$. En cada uno de los siguientes sumandos $p - 1$ de esta adición entra p con un exponente no inferior a α, y además, el coeficiente binomial que, en vigor del corolario del teorema 13, es divisible por p. Quiere decir que cada uno de estos sumandos también es divisible por $p^{\alpha+1}$. Por último, la diferencia $1 - 1 = 0$ puede ser suprimida. Por eso, según el teorema 6, $(a^{p^{\alpha}(p-1)} - 1) \vdots p^{\alpha+1}$. De tal modo queda analizado el caso en que el número m posee solamente un divisor primo.

Supongamos ahora que el teorema de Euler fue demostrado para los índices m_1 y m_2, siendo ellos primos entre sí. Demostremos este teorema para el índice $m = m_1 m_2$. Si luego admitimos que $m_1 = p_1^{\alpha_1} \ldots p_h^{\alpha_h}$ y $m_2 = p_{h+1}^{\alpha_{h+1}}$, entonces, con toda evidencia, nosotros obtenemos, precisamente, el paso inductivo indispensable para dar fin a la demostración del teorema. Así, demostremos la afirmación enunciada.

Sean los números a y m primos entre sí. Entonces lo serán, además, a y m_1. Quiere decir que $a^{\varphi(m_2)}$ y m_1 también son primos entre sí. Por eso, según hipótesis,

$$(a^{\varphi(m_2)})^{\varphi(m_1)} - 1 = a^{\varphi(m_1)\varphi(m_2)} - 1 = a^{\varphi(m_1 m_2)} - 1 = a^{\varphi(m)} - 1$$

es divisible por m_1. Exactamente de igual manera nos convencemos de que $a^{\varphi(m)} - 1$ es divisible también por m_2. Pero como los números m_1 y m_2 son primos entre sí, $a^{\varphi(m)} - 1$ es divisible además por su producto, o sea, por m. El teorema de Euler queda demostrado.

27. Sean

$$k_1 = \varphi(m) q_1 + r,$$
$$k_2 = \varphi(m) q_2 + r.$$

Entonces,

$$a^{k_1} = a^{\varphi(m) q_1 + r} = (a^{\varphi(m)})^{q_1} a^r.$$

A base de los teoremas de Euler y 20, $a^{\varphi(m) q_1} a^r$ es equirresidual con a^r en la división por m. De modo análogo se establece que en esta división son equirresiduales los números a^{k_2} y a^r. Esto significa que también los números a^{k_1} y a^{k_2} son equirresiduales en la división por m.

28. Hallemos al principio por lo menos una resolución (x', y') de esta ecuación. Evidentemente, para esto es sufi-

ciente encontrar tal número x' que $(ax' - c) \vdots b$. Por el teorema de Euler $(a^{\varphi(b)} - 1) \vdots b$. Quiere decir que $(ca^{\varphi(b)} - c) \vdots b$ y que el número $ca^{\varphi(b)-1}$ se puede tomar como x'.

Sean ahora (x'', y'') cualquier otra resolución de la ecuación $ax + by = c$. Mostremos que los números x' y x'' son equirresiduales en la división por b. En efecto, aceptemos que

$$ax' + by' = c,$$
$$ax'' + by'' = c.$$

Restando término por término la segunda igualdad de la primera obtenemos

$$a(x' - x'') - b(y' - y'') = 0,$$

de donde $a(x' - x'') \vdots b$. Como por condición a y b son primos entre sí, según el teorema 12 $(x' - x'') \vdots b$, y nos queda citar el teorema 19.

De tal modo, todos los valores conocidos de x se hallan entre los números

$$x_t = ca^{\varphi(b)-1} + bt.$$

Pero $(ax_t - c) \vdots b$, así que, suponiendo

$$y_t = \frac{-ax_t + c}{b} = c\,\frac{1 - a^{\varphi(b)}}{b} - at,$$

obtenemos que todas las parejas de números x_t e y_t son resoluciones de nuestra ecuación.

29. Considerando que m y 10 son primos entre sí, los números $10a + b$ y $(10a + b)\, 10^{\varphi(m)-1}$, según el teorema 15, resultan equidivisibles por m. Pero

$$(10a + b)\, 10^{\varphi(m)-1} = 10^{\varphi(m)} a + 10^{\varphi(m)-1} b,$$

así, de acuerdo a los teoremas de Euler y 20, $10a + b$ es equidivisible por m con el número $a + kb$.

1. $0 = a \cdot 0$ para cualquier a.

2. $a = 1 \cdot a$, quiere decir que $a \vdots 1$.

3. Sea $1 \vdots a$. Esto significa que para determinado entero c, $1 = ac$, de donde se deduce que $|a| \leqslant 1$. Y como $a \neq 0$, $a = 1$.

4. Es suficiente tomar cualquier $c > 1$ y poner $b = ac$.

5. En calidad de tal b se puede tomar, por ejemplo, $2a$. Sea en este caso que para determinado c también $2a \vdots c$ y $c \vdots a$. Así, hallaremos tales d_1 y d_2 que $2a = d_1 c$ y $c = d_2 a$. De aquí se deduce que $2a = d_1 d_2 a$ o, después de simplificar por a, que

$$2 = d_1 d_2.$$

Pero para los enteros d_1 y d_2 tal igualdad solamente es factible cuando uno de estos números es igual a 1 y el otro a 2. Si $d_1 = 1$, entonces $c = 2a = b$; pero si $d_2 = 1$, entonces $c = a$.

6. Las demostraciones no se diferencian en nada de las que se hacen en el caso de divisibilidad común.

7. Sea n un número fijo mayor que la unidad. Supongamos que $a \underset{n}{\vdots} b$ si hay un entero c tal que $a = bc$ y $c \leqslant n$. La justeza de los teoremas análogos a los 1, 3 y 4 se comprueba sin dificultad. No obstante, si admitimos que $a = nb$ y $b = nc$, entonces $a \underset{n}{\vdots} b$ y $b \underset{n}{\vdots} c$. En este caso $a = n^2 c$ y, dado que $n^2 > n$, la divisibilidad $a \underset{n}{\vdots} c$ no tiene lugar. Así, tampoco lo tiene $(a + a) \underset{n}{\vdots} b$.

8. a) Sean a_1 y a_2 dos números mínimos. Por la dicotomía, o bien $a_1 \geqslant a_2$, o bien $a_2 \geqslant a_1$. Si $a_1 \geqslant a_2$, entonces, debido a la pequeñez de a_1 tenemos $a_1 = a_2$. Si $a_2 \geqslant a_1$, entonces, debido a la pequeñez de a_2, tomamos $a_1 = a_2$.

b) Sean a un número determinado, b_1 y b_2 los dos inmediatos anteriores. Por la dicotomía, o bien $b_1 \geqslant b_2$, o bien $b_2 \geqslant b_1$. Para concretar aceptemos que $b_1 \geqslant b_2$. Nosotros tenemos que $a \geqslant b_1 \geqslant b_2$, y como el número b_2 es el inmediato anterior de a, o bien $b_1 = a$ o bien $b_1 = b_2$. Pero por requisito $b_1 \neq a$; quiere decir que $b_1 = b_2$ y la unicidad exigida queda demostrada.

c) Se llama número *inmediato posterior* de a a uno b, tal que $b \geqslant a$ y $b \neq a$, y de $b \geqslant c \geqslant a$ se deduce que o bien $c = b$, o bien $c = a$.

Supongamos que cierto a no tiene un número inmediato posterior. Esto significa que para cualquier $a_n \geqslant a$ y diferente de a, se hallará un a_{n+1} diverso tanto de a_n como de a, tal que $a_n \geqslant a_{n+1} \geqslant a$. Tomamos ahora un $a_1 \geqslant a$ arbitrario y distinto de a (en vigor de 2° esto se puede

hacer) y partiendo de él construyamos la sucesión infinita de números diversos

$$a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n \geqslant a_{n+1} \ldots \geqslant a.$$

La propia existencia de esta sucesión contradice a 4°. Por consiguiente, el número inmediato posterior existe. Aplicando la dicotomía se establece su unicidad, como se hizo en los puntos a) y b).

9. La propiedad transitiva (3°), lo ilimitado del conjunto de números (5°), la propiedad 4° y la existencia del número inmediato anterior (6°) siguen en vigor. La dicotomía se sustituye por *tricotomía* (o bien $a > b$, o bien $b > a$, o bien $a = b$).

La propiedad reflexiva (1°) resulta incorrecta, ya que $a > a$ nunca es cierto.

Por fin, lo que concierne a la afirmación 2° formalmente sigue en vigor (aunque, pudiera ser, que también nos parezca un tanto paradójico).

En efecto, rigurosamente hablando, esta afirmación en nuestro caso se formula así: para los números naturales cualesquiera a y b, de $a > b$ y $b > a$ se deduce que $a = b$.

Supongamos que esta enunciación no es cierta. Entonces hallaremos tales números naturales a y b que al mismo tiempo $a > b$, $b > a$ y $a \neq b$, cosa imposible. La contradicción obtenida demuestra que nuestra afirmación es correcta.

10. Admitamos un conjunto ordenado por la relación $\succeq$, poseedora de las propiedades 1°—7°. Como ya fuera establecido, el conjunto tiene un elemento mínimo. Llamémoslo a_0. De los resultados del problema 8 se deduce que cada elemento tiene su inmediato posterior. Designemos por a_1 el elemento que es inmediato posterior de a_0, por a_2 el que es inmediato posterior de a_1, etc. Como resultado obtenemos la sucesión

$$a_0, \ a_1, \ a_2, \ \ldots \qquad \text{(R.1)}$$

donde para cualquier n, $a_{n+1} \succeq a_n$. Del hecho que la relación $\succeq$ es reflexiva y transitiva se desprende que $a_i \succeq a_j$ única y exclusivamente cuando $i \geqslant j$. Nos queda mostrar que la sucesión (R.1) abarca todos los objetos examinados por nosotros. Esto se logra por inducción con un razonamiento muy sutil.

Supongamos que b_0 no pertenece a la sucesión (R.1). Consideraremos como primer paso de nuestro razonamiento por inducción la obtención de este b_0. Aceptemos haber efectuado n de sus pasos, a resultas de los cuales hemos obtenido determinado elemento b_{n-1}.

Si $b_{n-1} = a_0$, consideraremos terminado nuestro proceso; pero si $b_{n-1} \neq a_0$ entonces, el elemento b_{n-1} tiene un inmediato anterior, que para nosotros será, precisamente, b_n. En conclusión, obtenemos la sucesión de elementos diversos

$$b_0 \succeq b_1 \succeq b_2 \succeq \ldots \succeq b_n \succeq \ldots$$

A base de 4° esta sucesión deberá tener un término último. Pero por el mismo principio de su construcción tal término puede ser solamente a_0. Sea, para ser precisos, $b_n = a_0$.

No es difícil comprobar que si determinado a es el inmediato anterior de b, entonces b es el inmediato posterior de a. Quiere decir que $b_{n-1} = a_1$, b_{n-2}, $\ldots$ $b_0 = a_n$.

Lo último significa que b_0 pertenece a la sucesión (R.1), pero esto contradice a la hipótesis. Por consiguiente, la sucesión (R.1) contiene todos los objetos examinados por nosotros.

11. Sea a cierto número. Cualquier sucesión de números diversos $a_0 = a, a_1, a_2, \ldots, a_n$, para los cuales

$$a_0 \succ a_1 \succ a_2 \succ \ldots \succ a_n, \qquad \text{(R.2)}$$

donde a_n es mínimo, en el sentido de la ordenación $\succ$, será llamada *cadena de anteriores* de a_0; el número n se llama *longitud* de esta cadena.

Mostremos al principio que para las condiciones que nosotros le impusimos a la ordenación $\succ$, cada número concreto no puede tener cualquier cantidad de cadenas largas de anteriores.

En efecto, sea a determinado número y $b_1, b_2, \ldots b_k$, sus inmediatos anteriores.

Si a_1 no es inmediato anterior de a_0, a base de 9° podemos colocar en la cadena (R.2) un número que sea inmediato anterior de a. Por eso, si hay cadenas de anteriores de a tan largas como se quiera, deberán existir también tales cadenas de anteriores tan largas como se quiera que comiencen desde los números inmediatos anteriores de a. En adelante vamos a examinar solamente tales cadenas.

Cada cadena de anteriores de a es más larga exactamente en una unidad que cierta cadena de anteriores de uno de los números inmediatos anteriores. Si cada uno de ellos tuvieran cadenas de anteriores de longitud limitada, entonces el propio a no podría tener cadenas de anteriores tan largas como se quiera.

Quiere decir que para nuestra hipótesis, por lo menos uno de los números anteriores inmediatos de a_0 posee cadenas de anteriores tan largas como se quiera. Designémoslo por a_1 y repitamos, aplicando a él, todos los razonamientos que acabamos de hacer. Esto nos da cierto número a_2, anterior inmediato de a_1 que tiene cadenas de anteriores tan largas como se quiera. Repitiendo este proceso llegamos a la sucesión

$$a_0 \succ a_1 \succ a_2 \succ \ldots,$$

la cual, en vigor de 4°, tarde o temprano deberá cortarse. Esto significa que la sucesión va a tener tal término, al cual nuestros razonamientos ya no serán aplicables. Pero la aplicabilidad de los razonamientos a cada término subsiguiente de la sucesión ya fue establecida por nosotros. La contradicción obtenida muestra que ningún número posee cadenas de anteriores tan largas como se quiera.

Por consiguiente, para cada número a se puede elegir entre sus cadenas de anteriores la más larga. Designemos su longitud por $n(a)$. Si el anterior inmediato de b es a, entonces, evidentemente, $n(b) = n(a) - 1$, y para todos los a mínimos $n(a) = 0$.

Sea $A(a)$, por fin, un enunciado dependiente de a. Designemos por $B(n)$ el enunciado «$A(a)$ es cierta para todos los números a, para los cuales $n(a) = n$». Entonces, como es fácil de ver, la formulación del principio de inducción en la nueva forma para las afirmaciones $A(a)$ coincide con su formulación en la forma vieja para las afirmaciones $B(n)$.

12. a) Sean cuales fueran los números pares a y b, existen tales pares q y r, que

$$a = bq + r \quad (0 \leqslant r < 2b).$$

Estos números q y r son únicos.

Demostración. Dividimos residualmente a por $2b$, de la manera habitual:

$$a = 2bq + r \quad (0 \leqslant r < 2b) \qquad \text{(R.3)}$$

En este caso q y r son determinados unívocamente. De la paridad de a y $2bq$ se desprende la paridad de la diferencia de ellos, es decir, del número r. Nos queda, colocando que $2q = q'$, volver a escribir (R.3), en la forma

$$a = q'b + r \quad (0 \leqslant r < 2b)$$

y observar que ambos números q' y r son pares y se determinan de un solo modo.

13. Sea p el mínimo divisor primo del número a. De acá se deduce que $a = pb$. Cualquier divisor primo q del número b es también, al mismo tiempo, divisor de a. Por eso, $q \geqslant p$, o sea, también $b \geqslant p$, así, $a \geqslant p^2$, y, por fin, $p \leqslant \sqrt{a}$.

14. Sea $p_1, p_2, \ldots, p_k$ la relación completa de todos los números primos que entran, al menos, en una de las descomposiciones canónicas de a y b. Pongamos que

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}.$$

(Si a no es divisible por p_i, entonces $\alpha_i = 0$; si b no es divisible por p_i, entonces $\beta_i = 0$.) Sea γ_i el mayor de los números de α_i y β_i para $i = 1, 2, \ldots, k$, y δ_i el menor de ellos.

Entonces, a base del teorema 17, el máximo común divisor de a y b es $p_1^{\delta_1} \; p_2^{\delta_2} \ldots p_k^{\delta_k}$, y su mínimo común múltiplo,

$$p_1^{\gamma_1} \; p_2^{\gamma_2} \ldots p_k^{\gamma_k}.$$

15. Como se deduce del teorema 7, cada divisor del número a, con descomposición canónica $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, deberá adoptar la forma $p_1^{\beta_1}, \ldots, p_k^{\beta_k}$, donde β_1 toma los valores $\alpha + 1$: $0, 1, 2, \ldots, \alpha_1$; β_2, los valores $\alpha_2 + 1$, etc. Ya que son posibles cualesquiera combinaciones de estos valores y ellas nos dan todos los divisores de a, apareciendo cada uno una sola vez (si cualquier divisor se repitiera varias veces, significaría que él tiene varias descomposiciones canónicas), el número de tales divisores a es igual a

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1).$$

16. Admitamos que la descomposición canónica de a sea $p_1^{\alpha_1} p_2^{\alpha_2} \ldots$

... $p_k^{\alpha_k}$. Evidentemente, podemos poner que $p_1 = 2$, $\alpha_1 \geqslant 2$ y $p_2 = 3$, $\alpha_2 \geqslant 1$. Prosiguiendo, obtenemos:

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1) = 14,$$

de donde $k = 2$, $\alpha_1 + 1 = 7$ y $\alpha_2 + 1 = 2$. De tal modo, $a = 2^6 \cdot 3 = 192$.

17. Nosotros tenemos:

$$\tau(a^2) = \tau(p_1^{2\alpha_1} p_2^{2\alpha_2}) = (2\alpha_1 + 1)(2\alpha_2 + 1) = 81,$$

así que $(2\alpha_1 + 1)(2\alpha_2 + 1)$ es la descomposición del número 81 en dos factores. Como la numeración de los divisores simples de a depende de nosotros, limitémonos al examen de las siguientes posibilidades:

$$2\alpha_1 + 1 = 1, \qquad 2\alpha_2 + 1 = 81;$$
$$2\alpha_1 + 1 = 3, \qquad 2\alpha_2 + 1 = 27;$$
$$2\alpha_1 + 1 = 9, \qquad 2\alpha_2 + 1 = 9.$$

En el primero de estos casos $\alpha_1 = 0$, lo que contradice a la suposición de que el número α_1 es positivo. En los restantes,

$$\alpha_1 = 1, \qquad \alpha_2 = 13;$$
$$\alpha_1 = 4, \qquad \alpha_2 = 4.$$

Quiere decir que, o bien

$$\tau(a^3) = \tau(p_1^{3\alpha_1} p_2^{3\alpha_2}) = \tau(p_1^3 p_2^{39}) = (3+1)(39+1) = 160,$$

o bien,

$$\tau(a^3) = \tau(p_2^{3\alpha_1} p_2^{3\alpha_2} = \tau(p_1^{12} p_2^{12}) = 13 \cdot 13 = 169.$$

18. Sea $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ la descomposición canónica del número a. La condición del problema nos da

$$p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = 2(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1),$$

ó

$$\frac{p_1^{\alpha_1}}{\alpha_1 + 1} \frac{p_2^{\alpha_2}}{\alpha_2 + 1} \cdots \frac{p_h^{\alpha_h}}{k+1} = 2. \qquad (R.5)$$

Señalamos que

$$\frac{2^1}{1+1} = 1 < \frac{2^2}{2+1} = \frac{4}{3} < \frac{2^3}{3+1} = 2 < \frac{2^\alpha}{\alpha+1} \quad (\alpha \geqslant 4),$$

$$1 < \frac{3^1}{1+1} < 2 < \frac{3^\alpha}{\alpha+1} \quad (\alpha \geqslant 2),$$

$$2 < \frac{p^\alpha}{\alpha+1} \quad (p \geqslant 5,\ \alpha \geqslant 1).$$

Por eso, en el primer miembro de (R.5) cada quebrado no es inferior a uno y, naturalmente, ninguno mayor que dos. O sea, en el primer

miembro de (R.5) únicamente pueden haber quebrados del siguiente conjunto:

$$\frac{2^1}{1+1}, \frac{2^2}{2+1}, \frac{2^3}{3+1}, \frac{3^1}{1+1},$$

además, su producto es 2. Pero esto sólo ocurre en dos circunstancias: cuando en el primer miembro de (R.5) se halla solamente un quebrado, $\frac{2^3}{3+1}$, o dos, $\frac{2^2}{2+1}$ y $\frac{3^1}{1+1}$. Ambos casos corresponden a las dos respuestas del problema: 8 y 12.

19. Escribamos la descomposición canónica del número a:

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$

Entonces,

$$a^2 = p_1^{2\alpha_1} \dots p_k^{2\alpha_k},$$

y de acuerdo con (R.4) (problema 15)

$$\frac{\tau(a^2)}{\tau(a)} = \frac{(2\alpha_1+1)\dots(2\alpha_k+1)}{(\alpha_1+1)\dots(\alpha_k+1)}.$$

Es fácil ver que cada quebrado $(2\alpha_i+1)/(\alpha_i+1)$ crece (aproximándose a 2) con el aumento de α_i, de modo que el mínimo valor de este quebrado será alcanzado cuando $\alpha_i = 1$ y constituirá 3/2. Esto quiere decir que

$$\frac{\tau(a^2)}{\tau(a)} \geqslant \left(\frac{3}{2}\right)^k.$$

Está claro que siendo k suficientemente grande, $(3/2)^k > K$. Para esto basta con tomar

$$k > \frac{\log K}{\log 3/2}.$$

Por ejemplo, cuando $K = 100$, es suficiente tomar $k > 2/0{,}18 = 11{,}1$; como k tiene que ser entero, podemos tomar $k = 12$.

20. Para la división par, los teoremas análogos a los 11—14 dejan de ser ciertos. En efecto, los números 30 y 42 son primos en paridad. El mínimo par múltiplo es 420, y el producto, 1260.

Prosiguiendo, $60 = 6\cdot 10$ es divisible en paridad por el número 30 primo en paridad; 6 y 30 son primos en paridad entre sí, y 10 no es divisible en paridad por 30.

Por último, $60 = 6\cdot 10 = 30\cdot 2$ son dos descomposiciones distintas del número 60 en factores primos en paridad.

21. a) 116 es equirresidual con 4, y 17 con 1, en la división por 8. Quiere decir que A lo es con $5^{21} = (5^2)^{10}\cdot 5$. Pero en esta division, $5^2 = 25$ es equirresidual con la unidad. Por consiguiente, en la división por 8, A nos da el residuo 5.

b) 14 es equirresidual con —3 en la división por 17. Por eso A es equirresidual con $(-3)^{256} = 3^{256} = (3^3)^{85}\cdot 3$.

Pero 3^3 lo podemos sustituir por 10; $10^{85}\cdot 3 = (10^2)^{42} \times 30$. Luego, 10^2 es equirresidual con el número -2, y 2^4 con -1, en la división por 17. Quiere decir que A es equirresidual con $(-2)^{42}\cdot 30 = 2^{42}\cdot 30 = (2^4)^{10}\cdot 4\cdot 30 = (-1)^{10} \times 4\cdot 30 = 120$. Pero el último número al ser dividido por 17 da como residuo 1.

22. a) Sea n_1 el residuo de dividir n por 6. Entonces n_1 puede tomar los valores 0, 1, 2, 3, 4, y 5, mientras $n_1^3 + 11n_1$ es equirresidual con $n^3 + 11n$ en la división por 6. O sea, debemos probar la divisibilidad por 6 de los números 0, 12, 30, 60, 108 y 180. Todos ellos son divisibles por 6.

Para obtener el mismo resultado también es posible utilizar consideraciones más particulares. El número $n^3 + 11n$ es equirresidual con el $n^3 + 11n - 12n = n^3 - n = (n-1)\,n\cdot(n+1)$ en la división por 6. Pero de los tres números enteros sucesivos $n-1$, n y $n+1$, uno al menos es par (vale decir, es divisible por 2) y uno es divisible por 3 con exactitud. Esto significa (según el corolario del teorema 11) que el producto de estos tres números es divisible por 6. A propósito, hacemos notar que

$$\frac{1}{6}(n-1)\,n\,(n+1) = C^3_{n+1}.$$

b) Para $n \geqslant 2$ (empleando la fórmula del binomio):

$$4^n + 15n - 1 = (3+1)^n + 15n - 1 =$$
$$= 3^n + 3^{n-1}C_n^1 + \ldots + 3^2C_n^{n-2} + 3C_n^{n-1} + 1 +$$
$$+ 15n - 1 = 9\,(3^{n-2} + 3^{n-3}C_n^1 + \ldots + C_n^{n-2}) + 18n,$$

y ambos sumandos evidentemente, son divisibles por 9.

Para $n = 1$ nuestra expresión es igual a $4^1 + 15\cdot 1 - 1 = 18$.

c) La demostración se efectúa por inducción.

Para $n = 0$

$$10^{3^0} - 1 = 10^1 - 1 = 9 \text{ y } 3^{0+2} = 9.$$

Sea que ahora tiene lugar la divisibilidad

$$(10^{3^n} - 1) \,\vdots\, 3^{n+2}.$$

Entonces,

$$10^{3^{n+1}} - 1 = (10^{3^n})^3 - 1^3 = (10^{3^n} - 1)\,(10^{2\cdot 3^n} + 10^{3^n} + 1).$$

Por hipótesis de inducción el primer factor del segundo miembro es divisible por 3^{n+2}. Podemos sustituir los dieces del segundo factor por las unidades que en la división por 3 son equirresiduales con ellos; el número 3 obtenido muestra que el segundo factor es divisible por 3. Por consiguiente, todo el producto es divisible por $3^{n+3} = 3^{(n+1)+2}$, siendo esto precisamente lo que se pedía.

d) a^2 evidentemente es equirresidual con $a - 1$ en la división por $a^2 - a + 1$. Quiere decir que $a^{2n+1} + (a-1)^{n+2}$ es equirresidual con

$$a^{2n+1} + (a^2)^{n+2} = a^{2n+1} + a^{2n+4} = a^{2n+1}(1 + a^3) =$$
$$= a^{2n+1}(1 + a)(1 - a + a^2),$$

siendo justamente lo que se exigía.

e) $(n^k - 1) = (n - 1)(n^{k-1} + n^{k-2} + \ldots + n + 1)$.

f) $(n^{2l+1} + 1) = (n + 1)(n^{2l} - n^{2l-1} + \ldots - n + 1)$.

23. Sea $\sim$ una relación equivalente en el conjunto de números. Tomamos el número arbitrario a y examinamos todos los números que le son equivalentes. Como la relación $\sim$ es transitiva todos ellos son equivalentes entre sí. Designemos por K la clase de todos estos números.

Estudiemos ahora el número arbitrario b no perteneciente a K. Si fuera $b \sim c$, donde c es cierto número de K, entonces también sería $b \sim a$, lo que es imposible por la elección de b. Quiere decir que ninguno de los números ubicados fuera de K son equivalentes a ninguno de los que están en K. Por consiguiente, K es la clase de equivalencia que contiene a.

Dado que el número a fue tomado por nosotros absolutamente arbitrario, los razonamientos efectuados muestran que cada número pertenece a cierta clase de equivalencia. Esto es lo que, precisamente, se pedía.

24. No cabe duda que entre los números $0, 1, \ldots, m$ habrán dos pertenecientes a una misma clase. Sean ellos k y l: $k \sim l$. Hablando en general, tales parejas de números de una misma clase pueden incluso resultar varias. Elijamos aquella para la cual la magnitud $|k - l|$ sea máxima. Dado que $-l \sim -l$, por condición obtenemos

$$k - l \sim l - l = 0.$$

Luego, nosotros hallamos que también para cualquier n entero

$$n(k - l) \sim 0.$$

Por fin, para cualquier r

$$n(k - l) + r \sim r,$$

es decir, de $a \equiv b$ (mód. $k - l$) se deduce que $a \sim b$. De tal manera los tipos de relación $\sim$ contienen íntegramente a las clases de restos con respecto al módulo m.

Para que hubiera m clases de $\sim$ equivalentes es necesario que cada una de ellas contenga no más de un tipo de restos y que $k - l = m$.

25. a) Ambos miembros de la congruencia y el módulo son divisibles por un mismo número (se sobreentiende, diferente de cero).

En efecto,

$$ad \equiv bd \quad (\text{mód. } md)$$

significa que

$$ad - bd = (a - b)\, d \,\vdots\, md.$$

es decir, $(a - b) \,\vdots\, m$, de donde $a \equiv b$ (mód. m).

b) Ambos miembros de la congruencia pueden ser divididos por un número primo con el módulo.

Efectivamente, si d y m son primos entre sí, entonces, por el teorema 12, de

$$ad \equiv bd \quad (\text{mód. } m),$$

es decir, de $(a - b)\, d \,\vdots\, m$, se deduce que $a - b \,\vdots\, m$, lo que precisamente se requería.

26. Supongamos que

$$1 \leqslant k < l \leqslant p - 1, \quad ka \equiv la \quad (\text{mód. } p).$$

Esto significa que $(l - k)\, a \,\vdots\, p$. Por cuanto a no es divisible por p, $l - k \,\vdots\, p$. Lo cual tampoco puede ser, ya que $0 < l - k < p$.

27. **Necesidad.** Sea el número p primo. Tomemos $0 < q < p$. Entre los números $q, 2q, \ldots, (p - 1)\, q$ se hallará exactamente uno que al ser dividido por p nos dé como residuo la unidad. Aceptemos que tal número sea $\bar{q}q$:

$$\bar{q}q \equiv 1 \quad (\text{mód. } p). \qquad \text{(R.6)}$$

Por otro lado, entre los números $\bar{q}, 2\bar{q}, \ldots, (p - 1)\, \bar{q}$ también puede existir sólo uno que al ser dividido por p nos dé como residuo la unidad. Este, según fuera establecido, es $q\bar{q}$.

Aclaremos en qué casos $q = \bar{q}$. En todos estos casos la congruencia (28) se anota así:

$$q^2 \equiv 1 \quad (\text{mód. } p),$$

o lo que es lo mismo,

$$q^2 - 1 \equiv 0 \quad (\text{mód. } p).$$

Esto significa que

$$q^2 - 1 = (q + 1)\,(q - 1) \,\vdots\, p.$$

En vista de que el número p es primo, por el teorema 13 deberá ser o bien $(q + 1) \,\vdots\, p$, o bien $(q - 1) \,\vdots\, p$. Como q se halla entre cero y p, el primer caso es posible únicamente para $q = p - 1$, y el segundo, para $q = 1$. De tal modo, para $p = 2$ y $p = 3$ siempre será $q = \bar{q}$, mientras que para $p \geqslant 5$, solamente en los casos cuando $q = 1$ y $q = p - 1$.

Por consiguiente, para $p \geqslant 5$, todos los números restantes $2, \ldots, \ldots, p - 2$ pueden ser unidos en pares $(p - 3)/2$ tales, que el producto de los números componentes de cada uno de ellos, al ser divididos

por p, dejen como residuo 1. Anotemos la congruencia del tipo (R.6) para el total de dichos pares, agregando a esta lista la congruencia

$$p - 1 \equiv p - 1 \pmod{p},$$

y volvemos a multiplicar miembro a miembro todos los $(p-1)/2$ obtenidos de las congruencias.

Como resultado de esta multiplicación, en el primer miembro se obtiene el producto de todos los números desde 2 hasta $p - 1$, y en el segundo, $p - 1$:

$$2\cdot 3 \ldots (p-1) \equiv p - 1 \pmod{p},$$

o bien

$$1\cdot 2\cdot 3 \ldots (p-1) + 1 \equiv 0 \pmod{p}.$$

La última congruencia significa que

$$[1\cdot 2 \ldots (p-1) + 1] \vdots p,$$

y esto es precisamente lo que se exigía.

Quedan por verificar los casos cuando $p = 2$ y $p = 3$. Pero para ellos, evidentemente, $(1 + 1) \vdots 2$ y $(2 + 1) \vdots 3$.

Suficiencia. Si el número p no es primo podrá ser descompuesto en el producto de dos factores menores: $p = p_1 p_2$.

Si $p_1 \neq p_2$, entonces, p_1 y p_2 entran también como factores en el producto $1\cdot 2 \ldots (p-1)$ haciéndolo divisible por p_1p_2, es decir, por p. Aceptemos ahora que $p_1 = p_2 = q$. Entonces $p = q^2$ (o sea, p es el cuadrado de un número primo). Si $q > 2$ entonces $p > 2q$ y en el producto $1\cdot 2 \ldots (p-1)$ entran los factores q y $2q$, de modo que queda divisible por q^2, es decir, por p. En ambos casos $1\cdot 2 \ldots$ $\ldots (p-1) + 1$ no puede ser divisible por p. Para finalizar, si $p = 4$, entonces $1\cdot 2\cdot 3 - 1 = 5$, y por 4 no es divisible.

28. TEOREMA. *Sea $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ la descomposición canónica de m. Entonces, a fin de que los números A y B sean equirresiduales en la división por m, es necesario y suficiente que ellos lo sean en la división por $p_1^{\alpha_1}$, por $p_2^{\alpha_2}$, ..., por $p_k^{\alpha_k}$.*

Demostración. Necesidad. La equirresidualidad de A y B en la división por m significa que $(A - B) \vdots m$. Además, $(A - B) \vdots p_i^{\alpha_i}$ $(i = 1, \ldots, k)$ y los números A y B resultan equirresiduales en la división por todos los $p_i^{\alpha_i}$.

Suficiencia. Sean los números A y B equirresiduales en la división por cada uno de los $p_i^{\alpha_i}$. Designemos por r_i al residuo de la división de A y B por $p_i^{\alpha_i}$ $(i = 1, 2, \ldots, k)$. Esto significa que

$$A \equiv r_i \pmod{p_i^{\alpha_i}}. \qquad \text{(R.7)}$$

Supongamos que en adelante

$$\frac{m}{p_i^{\alpha_i}} = m_i, \quad i = 1, \ldots, k,$$

y multipliquemos el módulo y ambos miembros de la congruencia (R.7) por m_i:

$$Am_i \equiv m_i r_i \quad (\text{mód. } m).$$

Sumando miembro a miembro todas estas congruencias, obtenemos $A(m_1 + m_2 + \ldots + m_k) \equiv$

$$m_1 r_1 + m_2 r_2 + \ldots + m_k r_k \quad (\text{mód. } m). \qquad (\text{R.8})$$

Como A y B son equirresiduales en la división por $p^{\alpha 1}, p_2^{\alpha 2}, \ldots, p_k^{\alpha k}$, obtenemos también

$$B\,(m_1 + m_2 + \ldots + m_k) \equiv m_1 r_1 + \ldots + m_k r_k \quad (\text{mód. } m). \qquad (\text{R.9})$$

Restando miembro a miembro la congruencia (R.9) de la (R.8) resulta

$$(A - B(\,(m_1 + m_2 + \ldots + m_k r_k) \equiv 0 \quad (\text{mód. } m),$$

es decir, $(A - B)\,(m_1 + m_2 + \ldots + m_k) \equiv m$.

Pero la suma $m_1 + m_2 + \ldots + m_k$ y m son primos entre sí. En efecto, si ella tuviera con m un divisor común primo p él integraría la descomposición canónica de m, o sea, tendría la forma p_i. Pero entonces sería divisible por él tanto toda la suma como cada uno de los sumandos, a excepción de uno, el m_i, cosa imposible.

Ahora se puede aplicar el teorema 12, por el que $(A - B) \vdots m$, es decir, los números A y B son equirresiduales en la división por m.

29. a) Anotamos sistemáticamente todas las igualdades que describen las divisiones residuales que constituyen la aplicación del algoritmo de Euclides a los números a y b:

$$\left.\begin{array}{l} a = bq_0 + r_1, \\ b = r_1 q_1 + r_2, \\ r_1 = r_2 q_2 + r_3, \\ \ldots\ldots\ldots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, \\ r_{n-1} = r_n q_n. \end{array}\right\} \qquad (\text{R.10})$$

Nosotros tenemos que $r_{n-1} \vdots r_n$. Junto con $r_{n-2} = r_{n-1} q_{n-1} + r_n$, esto nos da que $r_{n-2} \vdots r_n$. Avanzando de modo análogo por el sistema de igualdades (R.10), hacia arriba nosotros obtenemos, por fin, que $a \vdots r_n$ y $b \vdots r_n$. O sea, que r_n es un divisor común de a y b.

Sea d cualquier divisor común de a y b. Junto con $a = bq_0 + r_1$ esto nos da que $r_1 \vdots d$. Avanzando por el sistema de igualdades (R.10) hacia abajo, nosotros obtendremos sucesivamente que $r_2 \vdots d$, $r_3 \vdots d$, ..., ..., $r_n \vdots d$. Quiere decir que r_n es divisible por cualquier divisor común de a y b, siendo por ello mismo su *máximo* común divisor.

b) La demostración se efectúa por inducción. Suponiendo $A_0 = 0$,

$B_0 = 1$, $A_1 = 1$, $B_1 = -q_0$, nosotros tenemos $r_0 = b = aA_0 + bB_0$ y $r_1 = aA_1 + bB_1$. Sean ahora

$$r_{k-1} = A_{k-1}a + B_{k-1}b,$$
$$r_k = A_k a + B_k b.$$

Pero, entonces,

$$r_{k+1} = r_{k-1} - r_k q_{k+1} = (A_{k-1} - q_{k+1}A_k)\,a + \\ + (B_{k-1} - q_{k+1}B_k)\,b,$$

y a nosotros nos queda poner

$$A_{k-1} - q_{k+1}A_k = A_{k+1},$$
$$B_{k-1} - q_{k+1}B_k = B_{k+1}.$$

A_n y B_n resultan los números A y B buscados.

30. Si b y c son primos entre sí, entonces, por lo expuesto anteriormente se pueden hallar tales enteros B y C que

$$bB + cC = 1$$

o, después de multiplicar por a,

$$abB + acC = a;$$

$ab \vdots c$ por condición; $ac \vdots c$ de manera evidente; o sea, también $a \vdots c$.

31. Limitémonos a examinar el criterio de residuos equivalentes al dividir por 8.

Presentemos el número natural arbitrario A en la forma $1000a + b$, donde $0 \leqslant b < 1000$ (es decir, b es el número trinario con el que termina A) y

$$f(A) = \\ = \begin{cases} b, & \text{si } A \geqslant 1000, \\ \text{al residuo de la división de } A \text{ por } 8, & \text{si } 8 \leqslant A < 1000, \\ \text{indeterminada}, & \text{si } A < 8. \end{cases}$$

32. Limitémonos a examinar el criterio de equirresidualidad, en el sistema duodecimal de numeración, para la división por 18.

Sea A presentado en la forma $144a + b$, donde $0 \leqslant b < 144$ (o sea, en el sistema duodecimal de numeración, b es la cifra binaria con la que termina el número A escrito en este sistema), y

$$f(A) = \\ = \begin{cases} b, & \text{si } a \geqslant 144, \\ \text{al residuo de la división de } A \text{ por } 18, & \text{si } 18 \leqslant A < 144, \\ \text{indeterminada}, & \text{si } A < 18. \end{cases}$$

La verificación de que el proceso de construcción de la sucesión A, $f(A)$, $f[f(A)]$, . . . realmente es un criterio de equirresidualidad, se efectúa de manera estándar.

33. Para aquellos m cuya descomposición canónica tiene el aspecto $2^\alpha \cdot 5^\beta$.

34 Las condiciones a) y b) se cumplen automáticamente. Por cuanto 10 y 1 son equirresiduales en la división por 3, también lo deberán ser los números A y $f(A)$. Por fin, el hecho de que para $A \geqslant 3$, $f(A) < A$, se establece con un cálculo sencillo.

35. a) $f(858\ 773) = 38$; $f(38) = 11$; $f(11) = 2$.

b) $f(A) = 4444 \cdot 4 = 17\ 776$; $f(17\ 776) = 28$; $f(28) = 10$; $f(10) = 1$

36. El criterio de residuos equivalentes al dividir por 9 es análogo al ya examinado de residuos equivalentes al dividir por 3.

A fin de obtener el criterio de residuos equivalentes al dividir por 11 presentamos el número A en la forma

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + \ldots + 10^2a_1 + a_0,$$

donde $0 \leqslant a_i < 100$. Evidentemente, tal exposición concuerda con la división de un número en «grupos» binarios (de derecha a izquierda). Sea

$$f(A) = \begin{cases} a_0 + a_1 + \ldots + a_n, & \text{si } A \geqslant 100, \\ \text{al residuo de la división de } A \text{ por } 11, & \text{si } 11 \leqslant A < 100, \\ \text{indeterminada}, & \text{si } A < 11. \end{cases}$$

Nos queda señalar que en la división por 11 los números A y $f(A)$ verdaderamente son equirresiduales y, además, $f(A) < A$.

Otro criterio de residuos equivalentes al dividir por 11 se obtiene presentando el número A en la forma

$$A = 10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10a_1 + a_0$$

y valiéndonos de la equirresidualidad de 10 con -1 y de 100 con 1 en la división por 11. Por eso A es equirresidual con el número $a_0 - a_1 + a_2 - a_3 + \ldots \pm a_n$, y la formulación del respectivo criterio de residuos equivalentes no presenta dificultad.

Por fin, dividiendo el número A en «grupos» trinarios, podemos presentarlo en la forma

$$10^{3n}a_n + 10^{3n-3}a_{n-1} + \ldots + 10^3a_1 + a_0$$

$(0 \leqslant a_i < 1000)$. Entonces, A es equirresidual con la suma $a_0 + a_1 + \ldots + a_n$ en la división por 37, y con la suma de signo variable $a_0 - a_1 + a_2 - \ldots \pm a_n$ en la división por 7, 11 y 13.

37. Como ejemplo examinemos el criterio de equirresidualidad para la división por 8, en el sistema ternario de numeración. Presentamos para esto un A arbitrario:

$$a_n3^{2n} + a_{n-1}3^{2(n-1)} + \ldots + a_13^2 + a_0, \text{ donde } 0 \leqslant a_i < 9.$$

Aquí, a_i es la esencia del grupo binario en que se fracciona al número A, contando de derecha a izquierda.

Nos queda suponer que

$$f(A) = \begin{cases} a_0 + a_1 + \ldots + a_n, & \text{si } A \geqslant 9, \\ 0, & \text{si } A = 8, \\ \text{indeterminada}, & \text{si } A < 8 \end{cases}$$

y efectuar los razonamientos estándar.

38. En el sistema de numeración de base 6 o compuesto de 6 guarismos: 5 $(k = 1)$, 7 $(k = 2)$, 43 $(k = 3)$;

En el sistema de numeración septenario: 2, 3, 6 $(k = 1)$, 4, 6, 12, 16, 24 $(k = 2)$; 171 $(k = 3)$;

En el sistema de numeración de base 9 o compuesto de 9 guarismos: 2, 4, 8 $(k = 1)$; 5, 10, 20, 40 $(k = 2)$; 7, 13, 14, 26, etc. $(k = 3)$;

En el sistema de numeración de base 13 o compuesto de 13 guarismos: 2, 3, 4, 6 $(k = 1)$; 7, 14, 21, etc. $(k = 2)$.

39. En el sistema de numeración ternario: 2, 4 $(k = 1)$; 8, 12, 24 $(k = 2)$; 13, 26 $(k = 3)$; 41 $(k = 4)$;

En el sistema de numeración quinario: 2, 3, 6 $(k = 1)$; 8, 12, 24 $(k = 2)$; 31 $(k = 3)$;

En el sistema de numeración octonario u octónico: 3,9 $(k=1)$, 5,13 $(k=2)$;

En el sistema de numeración decimal :11 $(k = 1)$; 101 $(k = 2)$; 7, 11, 13 $(k = 3)$.

40. Si los números a y b son equirresiduales, entonces $(a - b) \vdots m$. Por eso, en vigor del teorema 6, a y b son o no divisibles por m simultáneamente.

4 y 5 son equidivisibles pero no equirresiduales en la división por 3

41. Supongamos que de la equidivisibilidad por m se deduzca la equirresidualidad para la división por m. Esto significa que todos los números no divisibles por m tendrán el mismo residuo al ser divididos por él. Quiere decir que este residuo deberá ser igual a uno, así que $m = 2$.

42. La relación de equidivisibilidad por m, evidentemente, es reflexiva (cualquier número es equidivisible consigo mismo al ser divisible por m), simétrica (si a es equidivisible con b, entonces, b lo es con a) y transitiva (si a es equidivisible con b y b con c, entonces, a lo es también con c)

Por consiguiente, ésta es precisamente la relación de equivalencia. Aquí todos los números divisibles por m pertenecen a una clase y los que no, a otra.

43. Es fácil comprobar que cuando $m > 2$ la equidivisibilidad de las sumas no se deduce de la de los sumandos.

Para que la equidivisibilidad de los productos se desprenda de la de sus factores es necesario y suficiente que el número m sea primo.

En efecto, si uno de los productos es divisible por p primo, entonces, según el teorema 13, al menos uno de sus factores deberá ser divisible por él. Además, por p se divide un factor de otro producto que le es equidivisible y también, por lo tanto, todo el producto. Pero si un producto no es divisible por p, el otro tampoco lo será (de lo contrario, a base de lo que acabamos de establecer, también el primer producto sería divisible por p)

A la inversa, si el número p es compuesto, los productos de factores equidivisibles pueden no ser ya equidivisibles. Es suficiente poner $p = p_1p_2$ ($p_1 \neq 1$, $p_2 \neq 1$). Entonces, los números 1 y p_1, así como los números 1 y p_2 serán equidivisibles por p, mientras que los productos $1 \cdot 1$ y $p_1 \cdot p_2$, evidentemente, no

44. Corolario inmediato del problema 36.

45. El cumplimiento de las condiciones a) y b) es indudable.

Si en adelante $a - b \geq 0$, no cabe duda que $f(A) < A$. Pero si $a - 2b < 0$, entonces, esta desigualdad puede ser que no se cumpla. En este caso, el módulo $|a - 2b|$ alcanza su valor máximo cuando $a = 0$ y $b = 9$ y es igual a 18. Por

consiguiente, para $A \geqslant 19$, $f(A) < A$. La justeza de esta desigualdad para valores menores se asegura determinando la función f.

Por fin, $10a + b$ es equidivisible con $50a + 5b$ en la división por 7 (ya que 5 y 7 son primos entre sí) y, por lo tanto, con $50a + 5b - 7(7a + b) = a - 2b$.

46. El número 15, al ser dividido por 7, da 1 como residuo, y $1 - 2 \cdot 5 = -9$, da 5.

47. La condición c) $f(A) < A$ significa que $a + 4b < 10a + b$, o sea, $3b < 9a$. Por eso, para $a \geqslant 4$ la condición necesaria se cumple.

La condición d). Evidentemente en la división por 13, $10a + b$ es equidivisible con $40a + 4b$ y el último número es equirresidual con $a + 4b$.

48. El criterio de divisibilidad pierde eficiencia, ya que $f(39) = 39$.

49. Supongamos que es necesario construir el criterio de divisibilidad por cierto m. Procuremos elegir tal s, primo con m y en lo posible pequeño, que $(10s + 1) \vdots m$ (así ocurrió para $m = 7$; s resultó igual a 3), o bien $(10s + 1) \vdots m$ (por ejemplo, para $m = 13$, $s = 4$).

En el primero de estos casos, en la división por m, $A = 10a + b$ es equidivisible con

$$10as + bs = (10s + 1)a - a + bs,$$

es decir, con $a - bs$, y en el segundo, con

$$(10s - 1)a + a + bs,$$

es decir, con $a + bs$.

En relación a lo dicho, el número $10a + b$

en la división	por 17,	es	equidivisible con	$a - 5b$,
» »	» 19,	»	»	$a + 2b$,
» »	» 23,	»	»	$a + 7b$,
» »	» 29,	»	»	$a - 3b$,
» »	» 31	»	»	$a + 3b$,

La conclusión de las formulaciones exactas de estos criterios de divisibilidad se la dejamos al lector.

50. a) Como 100 es equirresidual con 2 en la divisón por 49, cualquier número de la forma

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + \ldots + 10^2 a_1 + a_0 \quad (0 \leqslant a_i < 100)$$

es equirresidual con

$$2^n a_n + 2^{n-1} a_{n-1} + \ldots + 2a_1 + a_0$$

en la división por 49.

b) $10a + b$ es equidivisible con $a + 5b$ en la división por 49.

51. Evidentemente, para $A \geqslant 6$, tendremos $f(A) < A$.

52. a) La presentación de A dentro del sistema de numeración septenario, en la forma $7a + b$, da su equidivisibilidad con $a + 3b$ en la división por 5;

b) La presentación de A dentro del sistema de numeración de base 11 o compuesto de 11 guarismos, en la forma $11a + b$, da su equidivisibilidad con $a + 2b$ en la división por 7;

c) La presentación de A dentro del sistema de numeración duodecimal, en la forma $12a + b$, da su equidivisibilidad con $a - 7b$ en la división por 17.

53. Las condiciones a) y b) se cumplen automáticamente. Las c) y d) son observadas porque el paso de A a $F(A)$ se reduce a sustituir ciertos números por sus residuos de la división entre A (menores que los mismos números y equirresiduales con ellos).

54. a) $r_2 = r_3 = \ldots = r_n = 0$, es decir, $r_k = 0$ $(k \geqslant 2)$;

b) $r_3 = r_4 = \ldots = r_n = 0$, es decir, $r_k = 0$ $(k \geqslant 3)$.

c) $r_1 = r_2 = \ldots = r_n = 1$, es decir, $r_k = 1$;

d) $r_1 = r_3 = \ldots = r_{2t-1} = -1$, $r_2 = r_4 =$
$= \ldots = r_{2t} = 1$, es decir, $r_k = (-1)^k$;

e) $r_{6t+5} = 3$, $r_{6t+2} = 2$, $r_{6t+3} = 6$, $r_{6t+4} = 4$,
$r_{6t+5} = 5$, $r_{6t} = 1$.

55. Se la dejamos al lector.

56. Tomamos un m arbitrario y ponemos que

r_1 es igual al residuo de la división de t por m,
r_2 » » » » » » » » tr_1 por m, etc.

Entonces el número

$$a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$$

es equirresidual con

$$a_n r_n + a_{n-1} r_{n-1} + \ldots + a_1 r_1 + a_0,$$

en la división por m. Luego de esto, la construcción del criterio exigido no presenta dificultad.

57. Se lo dejamos al lector.

58. $10^2 = 7 \cdot 14 + 2$, de modo que $r = 2$ y entonces tenemos que $A_0 = 1048576$, $A_1 = 1 \cdot 2^3 + 4 \cdot 2^2 + 85 \cdot 2 +$

$+ 76 = 270$, $A_2 = 2 \cdot 2 + 70 = 74$ y $A_3 = 4$.

59. Si en la división por m, t es equirresidual con $r = r_1$, entonces, en la división por dicho número,

$$tr_1 \text{ es equirresidual con } r^2 = r_2,$$
$$tr_2 \text{ » » » } r^3 = r_3,$$

etc.

60. Ni $2^4 - 2$, ni $2^3 - 1$ son divisibles por 4.

61. Si $a \vdots p$, entonces $a^p \vdots p$, y el teorema queda demostrado. Pero si a no es divisible por p, entonces a y p son primos entre sí y es posible simplificar la congruencia expuesta en la condición del teorema:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Para comprobar la última congruencia dividimos residualmente por p cada uno de los números del tipo ta ($t = 1, 2, \ldots, p-1$):

$$ta = q_t p + r_t$$

Esto puede ser escrito así:

$$\left.\begin{array}{l} a \equiv r_1 \pmod{p}, \\ 2a \equiv r_2 \pmod{p}, \\ \ldots\ldots\ldots\ldots\ldots \\ (p-1)\, a \equiv r_{p-1} \pmod{p}. \end{array}\right\} \qquad \text{(R.11)}$$

Del resultado del problema 26 se desprende que entre los números r_1 encontramos exactamente una sola vez cada uno de los números $1, 2, \ldots, p-1$. Multiplicando toda la congruencia obtenemos

$$1 \cdot 2 \ldots (p-1)\, a^{p-1} \equiv 1 \cdot 2 \ldots (p-1) \pmod{p}.$$

Nos queda simplificar esta congruencia por $1 \cdot 2 \ldots (p-1)$.

62. $\varphi(12) = \varphi(2^2 \cdot 3) = 2^{2-1}(3-1) = 2 \cdot 2 = 4$,

$\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 2^{3-1}(3-1)(5-1) = 4 \cdot 2 \cdot 4 = 32$,

$\varphi(1000) = \varphi(2^3 \cdot 5^3) = 2^{3-1}5^{3-1}(5-1) = 4 \cdot 25 \cdot 4 = 400$.

63. Vamos a buscar m en la forma $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_h^{\alpha_h}$. Entonces,

a) $p_1^{\alpha_1-1}(p_1-1)\, p_2^{\alpha_2-1}(p_2-1) \ldots p_h^{\alpha_h-1}(p_h-1) = 10$.

El producto del primer miembro deberá ser divisible por 5.

Quiere decir, o bien que uno de los números $p_1, p_2, \ldots$ $\ldots, p_k$ es 5 (para ser exactos pongamos $p_1 = 5$), o bien que por 5 es divisible una de las diferencias $p_1 - 1, p_2 - 1, \ldots$ $\ldots, p_k - 1$ (supongamos que para esta circunstancia $(p_1 - 1) \vdots 5$). En el primero de estos casos $p_1 - 1 = 4$, cosa imposible, ya que 10 no es divisible por 4. En el segundo, por cuanto p_1 deberá ser número primo y $10 \vdots (p_1 - 1)$, únicamente es posible para $p_1 = 11$. Pero entonces $\alpha_1 = 1$, y del teorema 25 se deduce que

$$\varphi\left(\frac{m}{11}\right) = 1,$$

es decir, o bien $\frac{m}{11} = 1$, o bien $\frac{m}{11} = 2$.

En conclusión, nosotros tenemos que $m_1 = 11$ y $m_2 = 22$.

b) $p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_k^{\alpha_k - 1}(p_k - 1) = 8.$

Si m es impar, entonces $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 1$ (pues el segundo miembro de la desigualdad anotada es la potencia de dos):

$$(p_1 - 1)(p_2 - 1) \ldots (p_k - 1) = 8.$$

Esto es posible únicamente, cuando $k = 2$, $p_1 = 3$ y $p_2 = 5$, es decir, cuando $m = 15$.

Sea ahora el número m par. Supongamos, para certeza, que $p_1 = 2$. Indudablemente, $\alpha_2 = \ldots = \alpha_k = 1$ como antes y nosotros tenemos que

$$2^{\alpha - 1}(p_2 - 1) \ldots (p_k - 1) = 8.$$

Es evidente que $\alpha \leqslant 4$. Si $\alpha = 1$, entonces, el caso se asemeja al examinado: así, la desigualdad escrita es solamente posible para $k = 3$, $p_2 = 3$ y $p_3 = 5$, es decir, para $m = 30$.

Si $\alpha = 2$, entonces $k = 2$, $p_3 = 5$ y $m = 20$.

Si $\alpha = 3$, entonces $k = 2$, $p_2 = 3$ y $m = 24$.

Si, por fin, $\alpha = 4$, entonces $k = 1$ y $m = 16$.

Así, las resoluciones de nuestros problemas son:

$$m_1 = 15,\ m_2 = 30,\ m_3 = 20,\ m_4 = 24 \text{ y } m_5 = 16.$$

64. Supongamos que

$$p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_k^{\alpha_k - 1}(p_k - 1) = 14.$$

Cada uno de los números del tipo $p_i - 1$ es o bien la unidad, o bien un número par, y por eso no puede ser siete. Habiendo de ser menor que el número primo en una unidad, tampoco podrá ser igual a 14. Quiere decir que uno de los números $p_i^{\alpha_i-1}$ es siete. Pero entonces, $p_i - 1 = 6$ y 14 no es divisible por 6.

65. Sea $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Examinemos al principio el caso cuando m es potencial de un número primo: $m = p^\alpha$. A fin de que cierto número y m sean primos entre sí es necesario y suficiente que este número no sea divisible por p. Pero entre los números 0, 1, 2, . . ., $m - 1$ existen solamente $\frac{m}{p}$ números divisibles por p. Por consiguiente, en esta notación, habrá

$$m - \frac{m}{p} = m\left(1 - \frac{1}{p}\right) = p^\alpha\left(1 - \frac{1}{p}\right) = p^{\alpha-1}(p-1) = \varphi(m).$$

números primos con p.

Señalemos ahora que para que a y m sean primos entre sí es necesario y suficiente que con a sea primo el residuo de la división de a por m.

Por lo que acabamos de establecer, la cantidad de residuos de la división por $p_i^{\alpha_i}$, recíprocamente primos con $p_i^{\alpha_i}$, es igual a $\varphi(p_i^{\alpha_i})$. Pero, como ya fue explicado en el proceso de resolución del problema 40, de la equirresidualidad de los números para la división por todos los $p_i^{\alpha_i}$, se deduce su equirresidualidad en la división por m y viceversa. Además, si queremos que un número sea primo con m, es necesario y suficiente que lo sea con cada uno de los números $p_i^{\alpha_i}$. Por consiguiente, a cada combinación de los residuos de la división por $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$, primos con los respectivos divisores, le corresponde exactamente un residuo de la división por m, primo con m. También es necesario señalar que la cantidad de tales combinaciones de residuos es igual a $\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k}) = \varphi(m)$.

66. Tenemos

$$a_1 = A + q_1 m_1 \text{ y } a_2 = A + q_2 m_2.$$

Por eso

$(a_1 m_2 + a_2 m_1)(m_1 + m_2)^{\varphi(m_1 m_2) - 1} =$

$$= [A(m_1 + m_2) + (q_1 + q_2) m_1 m_2] (m_1 + m_2)^{\varphi(m_1 m_2) - 1} =$$
$$= A(m_1 + m_2)^{\varphi(m_1 m_2)} + (q_1 + q_2) m_1 m_2 (m_1 + m_2)^{\varphi(m_1 m_2) - 1}.$$

Aquí, según el teorema de Euler, en la división por $m_1 m_2$ el primer sumando es equirresidual con A, y el segundo, divisible por $m_1 m_2$. Eso significa que al dividir por $m_1 m_2$, toda la suma es equirresidual con A.

67. Se lo dejamos al lector.

68. » » » » »

69. » » » » »

70. $n^{13} - n = n(n^{12} - 1)$. Pero

$$n^{12} = n^{\varphi(13)} = n^{2\varphi(7)} = n^{3\varphi(5)} = n^{6\varphi(3)} = n^{12\varphi(2)}.$$

Por eso, o bien $n \vdots p$, o bien $(n^{12} - 1) \vdots p$ para $p = 2, 3, 5, 7, 13$. Ahora es preciso remitirse al teorema 16.

71. Se lo dejamos al lector.

72. » » » » »

73. Sea d el máximo común divisor de los números c y b. Si c no es divisible por d, entonces, la ecuación $ax + by = c$ no tiene solución en números enteros. Pero si lo es, entonces ambos miembros de la ecuación pueden simplificarse por d y nosotros llegamos a un caso ya examinado.

74. Sean A y B tales que $aA + bB = 1$. Supongamos que

$$x_t = cA + bt,$$
$$y_t = c\frac{1 - aA}{b} - at.$$

Entonces,

$$ax_t + by_t = a(cA + bt) + b\left(c\frac{1 - aA}{b} - at\right) =$$
$$= caA + abt + c(1 - aA) + abt = c,$$

y (x_t, y_t) es verdaderamente la solución de nuestra ecuación.

75. a) $x_t = 9 \cdot 5^5 + 7t = 28\,125 + 7t,$

$$y_t = 9\frac{1 - 5^6}{7} - 5t = -20\,088 - 5t.$$

Por cuanto los términos independientes y coeficientes que acompañan a t en las expresiones para x_t e y_t son, al decir, «aproximadamente proporcionales», nosotros espera-

mos obtener nociones de nuestras resoluciones en números menores. En efecto, podemos escribir

$$x_t = 6 + 7\,(t + 4017),$$
$$y_t = -3 - 5\,(t + 4017)$$

o, suponiendo que $t + 4017 = t'$, nosotros obtenemos

$$x_{t'} = 6 + 7t',$$
$$y_{t'} = -3 - 5t'.$$

Señalamos que el procedimiento de resolución de ecuaciones en números enteros, expuesto en el problema 74, permite utilizar números menores, aunque también exige cálculos algo más complejos.

b) Hagamos valer que 25, por el módulo 13, pertenece al índice 2. Podemos escribir

$$x_t = 8\cdot 25 + 13 = 200 + 13t,$$
$$y_t = 8\,\frac{1-25^2}{13} - 25t = -384 - 25t$$

o, después de simplificar,

$$x_{t'} = 5 + 13t',$$
$$y_{t'} = -9 - 25t'.$$

76. La condición c) se asegura automáticamente y la d) se deduce del teorema 25.

77.

m	17	19	27	29	31	49
k'	12 (ó 5)	2	19	3	28 (ó -3)	5

78. Se lo dejamos al lector.

79. Se lo dejamos al lector.

80. a) $8^{\varphi(21)-1} = 8^{11} = 64^5\cdot 8$. En la división por 21 este número es equirresidual con 8. Quiere decir que $8a + b$ y $a + 8b$ son equidivisibles en la división por 21.

b) $12^{\varphi(31)-1} = 12^{29} = (12^2)^{14}\cdot 12 = 144^{14}\cdot 12$ es equirresidual con $11^{14}\cdot 12 = 121^7\cdot 12 = (-3)^7\cdot 12 = -(3^3)^2\cdot 3\cdot 12 = -(31-4)^2\,(31+5)$, en la división por 31 y también equirresidual con $-16\cdot 5 = -80$. El último número, evidentemente, es equirresidual con 13. Por lo tanto, los números $12a + b$ y $a + 13b$ son equidivisibles en la división por 31.

LECCIONES POPULARES DE MATEMÁTICAS

«Lecciones populares de matemáticas» es una colección que se inició en 1975 y lleva publicados hasta el momento cerca de 50 folletos. Escritas por matemáticos soviéticos famosos, tanto por su labor docente como por su obra científica, dedicadas a temas interesantes de Matemáticas Elementales o intermedias entre ésta y la Matemática Superior expuestas en forma clara y precisa, que como regla no exige conocimientos previos especializados, las «Lecciones» están destinadas a un amplio círculo de lectores y pueden compararse a pequeños yates que brindan la posibilidad de realizar, bajo el mando de capitanes expertos, un corto y agradable viaje por el inmenso océano de la ciencia matemática, bien en la proximidad de las costas, bien adentrándose en aquél. Al mismo tiempo, las «Lecciones» estimulan en el lector el don del razonamiento lógico y la aptitud de descubrir relaciones entre fenómenos aparentemente muy alejados, familiarizándole con los elementos principales de la cultura matemática. Por todo ello, las «Lecciones», destinadas en un principio a los alumnos de los grados superiores de la enseñanza media, pueden ser recomendadas también a los estudiantes de cualquier especialidad y no dejan de tener interés para los maestros y profesionales.

Los libros de esta serie tratan, como regla, sobre temas especiales de las Matemáticas y, por consiguiente, están destinados a un círculo muy restringido de lectores que, aparte de los profesionales, abarca a los estudiantes de los Institutos Politécnicos y de las Facultades de Ciencias Naturales de las universidades. Pueden ser recomendados como material adicional de estudio al tratar determinados temas del programa y también pueden ser aprovechados en el trabajo de los círculos matemáticos. Los maestros encontrarán al leerlos algunos momentos que sin duda podrán ser tratados en los círculos matemáticos escolares.

A NUESTROS LECTORES

Nikolski S.

ELEMENTOS DEL ANÁLISIS MATEMÁTICO

Este libro está escrito para ayudar a los escolares que estudian el análisis matemático, así como a los maestros de escuela secundaria que dan clases de dicha asignatura. La obra también será útil para los alumnos de escuelas de peritaje, e incluso para la autodidáctica o el repaso de la materia del análisis matemático al nivel de las exigencias que se presentan en escuelas respecto a esta disciplina.

Los capítulos primero y segundo son los básicos, están dedicados al análisis matemático y pueden considerarse por separado de los demás, como independientes. En los primeros dos capítulos el análisis matemático se estudia a base de la geometría y la física. La gráfica continua y el movimiento, por sí mismos, sirven de fundamento para las deducciones básicas. Se da una idea del límite de una sucesión y del de una función. Se exponen el cálculo diferencial e integral y sus aplicaciones. En el tercer capítulo se estudia la noción de los números reales. El capítulo cuarto está dedicado a la fórmula del binomio de Newton y al análisis combinatorio. En el último, quinto, capítulo, el lector encontrará una breve información acerca de los números complejos y su papel al resolver ecuaciones algebraicas.

Lecciones populares de matemáticas

Obras de nuestro sello editorial

V.A. Uspenski
Algunas aplicaciones de la mecánica a las matemáticas

Yu.I. Lyúbich, L.A. Shor
Método cinemático en problemas geométricos

N.Ya. Vilenkin
Método de aproximaciones sucesivas

V.G. Shervátov
Funciones hiperbólicas

A.S. Solodóvnikov
Sistemas de desigualdades lineales

Editorial MIR



Moscú